Aite Novarica

MARCH 2022

SCAMS

ON THE PRECIPICE OF THE SCAMPOCALYPSE

TRACE FOOSHÉE

This report is provided compliments of:

callsign®

IMPACT REPORT

IMPACT REPORT

MARCH 2022

SCAMS

On the Precipice of the Scampocalypse

TRACE FOOSHÉE

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

IMPACT POINTS

- This Impact Report examines recent trends in scam activity based largely on observations from interviews with 18 fraud executives and a survey of 32 financial institutions (FIs). It examines how scams are categorized, how those definitions impact regulation and reimbursement policies, and how FIs are mobilizing to address the risk of scams.
- The U.K. market has been struggling with managing the disruptive influence of scams for almost a decade. As a result, they have established a useful taxonomy for defining and measuring scams, which has helped them mobilize the industry, regulators, and legislators to collaborate on tackling the problem holistically.
- As useful as the taxonomy is, and as helpful as the Federal Reserve Banks' Fraud Classifier Model is, both fall short in distinguishing between scams that seek to reveal sensitive information and those meant to induce the victim to make an authorized payment.
- The scale of scam activity is on the rise globally. It recently marked the grim milestone of surpassing card fraud losses in the U.K. The rates of growth in the U.S. market are widely distributed.
- Evidence for the driving forces behind the increase in scam activity points to increases in the ranks of new fraudsters that are less technically proficient than their more seasoned peers. These findings are supported by widespread reports of social engineering attack patterns.
- Recently published bulletins from the Consumer Financial Protection Bureau (CFPB) reveal that the U.S. regulator intends to take a harder line on enforcing how FIs structure their reimbursement policies to conform with the Electronic Funds Transfer Act and Regulation E. These bulletins do not directly apply to scams that seek to induce the victim into authorizing a payment. Still, they are expected to materially impact how FIs manage reimbursements for scams resulting in account takeovers.
- Demand for innovation in solutions that can be applied to detecting and preventing scams will begin to emerge. This demand will drive solution providers (particularly decision analytics platforms, orchestration hubs, and signal detection systems) to evolve their offerings further down the path of more nuanced capacities to predict anomalous patterns of interactions and transactions.

Introduction

Fraud is an interesting topic no matter how you look at it, but the most interesting instances are the edge cases. The edge cases are the kinds of fraud that exist on the periphery of policies shaped by regulatory requirements and market forces. They include topics like synthetic identity fraud, mule activity, and scams.

Historically, scams have been a relatively minor irritation for most fraud executives, but that began to change about 10 years ago when fraudsters began industrializing business email compromise (BEC) attacks on corporate banking customers. Scams targeting consumers picked up steam in the U.K. shortly after that market rolled out its Faster Payment Service. Today, the U.K. market is nearly saturated with scam activity, and fraudsters are rapidly replicating this successful tactic in countries across the globe as they enable faster payment rails.

Should the rate of scam activity reach the same proportional levels in North America as \ in the U.K., it’s reasonable to expect significant disruptions in the form of increased regulatory pressure and a deterioration in consumer sentiment in the wake of such a trend.

This report examines how scams are defined and categorized and investigates trends in scam activity in the U.K. and North America through late 2021. The report examines how patterns of scam activity developed and ultimately led to notable changes to reimbursement policies and control frameworks in the U.K. It considers indications from regulators in the U.S. market of potential shifts in how reimbursement policies might follow similar patterns as they did in the U.K. market. The report also examines how FIs are mobilizing to mitigate the increased risk of scam activity.

Methodology

The research supporting this report is informed by interviews with 18 North American fraud executives from 17 FIs with over US$30 billion in assets between August and October 2021. Additional insights were provided from a survey of 32 North American fraud executives who attended Aite-Novarica Group’s 2021 Financial Crime Forum in September 2021. Given the size and scope of the research sample, this report’s data offers a directional indication of conditions in the market.

SCOPE AND SCALE OF SCAMS

Scams occupy a unique space in the minds of fraud professionals. Everyone agrees that a scam is a form of fraud, of course, but there is a good deal of divergence of thought beyond that. In its simplest form, an attacker uses deception to overcome security controls to compel the victim to reveal sensitive information later used to steal money or send money to the attacker or a confederate of the attacker. What makes scams different from other forms of fraud is the degree to which the circumstances of the scam influence liability if the parties involved are unable to recover the funds. Fraud professionals, the banking public, and regulators diverge insofar as it shapes claims outcomes.

This alone is a sufficient reason to deconstruct scams and create a conceptual model for categorizing and characterizing them. However, there is another equally important reason to do so. If fraud professionals can't agree on a consistent way to define and categorize scams, then the important task of measuring the frequency, distribution, and severity of the event will fail to reveal any meaningful trends. These trends, if left unchecked, could grow to a scale that could eventually result in profound damage to the foundational trust relationship upon which the institution of banking rests.

Developing a conceptual model for scams and defining them is a helpful prerequisite to understanding more about the scope and scale of the problem. It is necessary to explore the implications of the trend and why leaders throughout the industry need to pay close attention to it to avoid the unintended consequences of inaction. As the saying goes, "If you can't measure it, you can't fix it." And reaching an agreement with regulators and customers around how to resolve disputes related to scams is something FIs must contend with.

THE CASE FOR MORE STRUCTURED THINKING ABOUT SCAMS

A useful perspective to take when considering scams is to envision them from the fraudster's point of view. First, consider that the overriding objective for the fraudster is to get money out of the victim's account and into a place where the funds are sheltered from recovery efforts. Fraudsters must have a plan of attack to accomplish this. That plan of attack can, of course, take many different forms, but they all boil down to one of the three basic patterns of attack listed in Table A.

TABLE A: PATTERNS OF ATTACK

ATTACK	DESCRIPTION
Instrument fraud	The fraudster seeks to steal money from the victim by gaining control of one or more payment instruments, such as a card or check, and then making unauthorized payments with that instrument.
Account takeover	The fraudster seeks to steal money from the victim by gaining control of the account in such a way that enables them to make an unauthorized transfer, a payment, or an exchange of the account contents.
Payment scam	The fraudster seeks to steal money from the victim by deceiving an authorized user of the account into authorizing a transfer, a payment, or an exchange of the account contents.

Source: Aite-Novarica Group

Perhaps the most important concept cited in the definitions of attacks in Table A is "authorization." The notion of whether a payment or transfer of funds is authorized or unauthorized is pivotal to understanding how to categorize the attack and how FIs, their customers, and regulators diverge in the matter of liability in the event of a dispute.[1]

Classifying Scams

Beyond some foundational characteristics, fraud executives, particularly in the U.S. market, use various terms, definitions, and descriptions to classify and conceptualize what they include under the term "scam." It's helpful to contrast the differences between the way FIs in the U.K. market articulate and report on scams and adjacent forms of fraud and how FIs in other markets do.

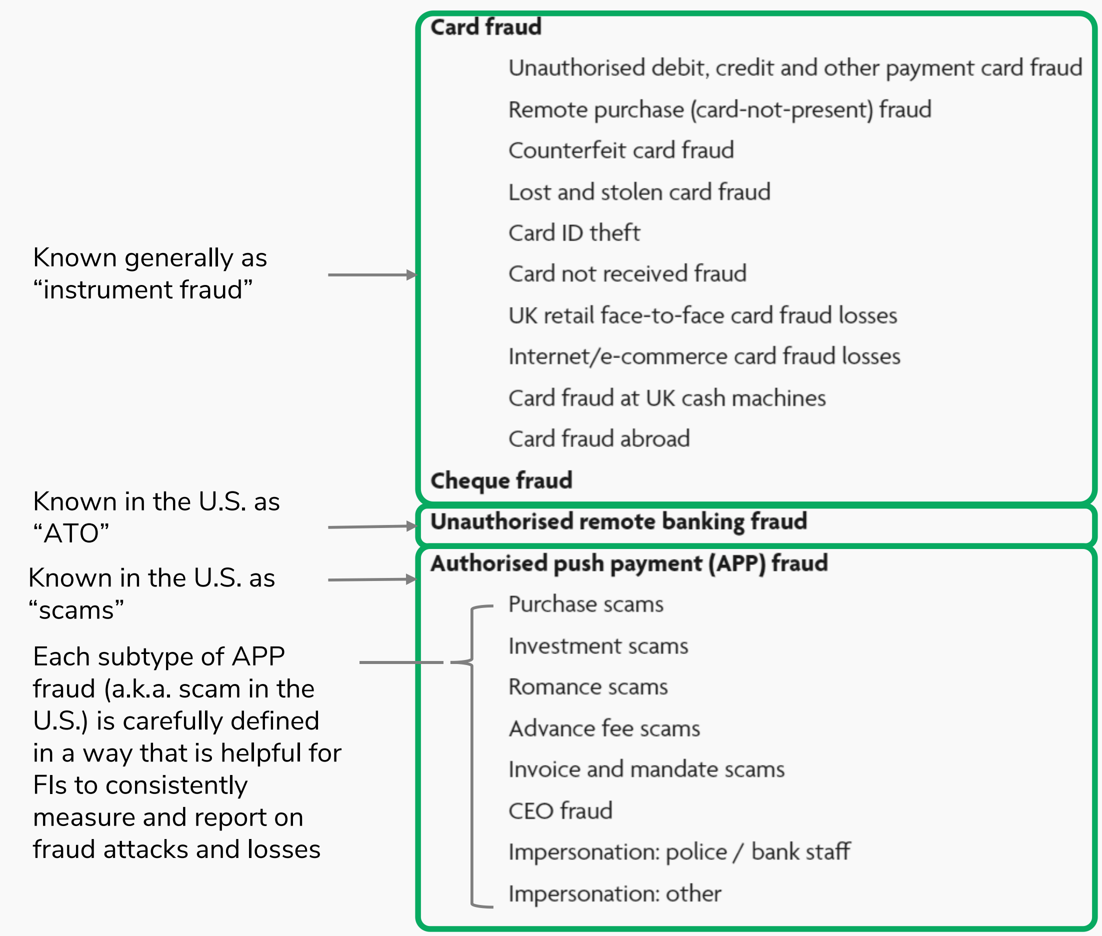
FIs in the U.K. market have a much more structured, consistent, and disciplined taxonomy than those in other markets. The terms FIs in the U.K. use to differentiate between types of fraud are precise, descriptive, and consistent. For example, fraud executives in the U.K. use the terms "authorized push payments" and "unauthorized

[1] For the sake of simplicity, it is assumed that the fraudster is attacking a credit or monetary account as opposed to a cash-equivalent account, such as a customer loyalty rewards account. The conceptual model works just as well for illustrating similar kinds of attacks on accounts that hold cash equivalents that can be exchanged as opposed to transferred or funneled through a payment network.

remote banking fraud” to differentiate between fraud resulting from an authorized party and fraud from an unauthorized party. Practitioners in other markets use “scams” and “ATO” to distinguish whether an authorized or unauthorized party issued the instructions.

U.K. Finance, the primary financial services trade association in the U.K., maintains the taxonomy for defining fraud in collaboration with member FIs. Part of that taxonomy includes detailed definitions for specific subtypes of fraud attacks. These subtypes are useful in establishing a consistent and enforceable standard that FIs can adhere to when reporting fraud losses (Figure 1).

FIGURE 1: U.K. FINANCE’S FRAUD TAXONOMY



Known generally as “instrument fraud”

Card fraud

- Unauthorised debit, credit and other payment card fraud
- Remote purchase (card-not-present) fraud
- Counterfeit card fraud
- Lost and stolen card fraud
- Card ID theft
- Card not received fraud
- UK retail face-to-face card fraud losses
- Internet/e-commerce card fraud losses
- Card fraud at UK cash machines
- Card fraud abroad

Cheque fraud

Known in the U.S. as “ATO”

Unauthorised remote banking fraud

Known in the U.S. as “scams”

Authorised push payment (APP) fraud

- Purchase scams
- Investment scams
- Romance scams
- Advance fee scams
- Invoice and mandate scams
- CEO fraud
- Impersonation: police / bank staff
- Impersonation: other

Each subtype of APP fraud (a.k.a. scam in the U.S.) is carefully defined in a way that is helpful for FIs to consistently measure and report on fraud attacks and losses

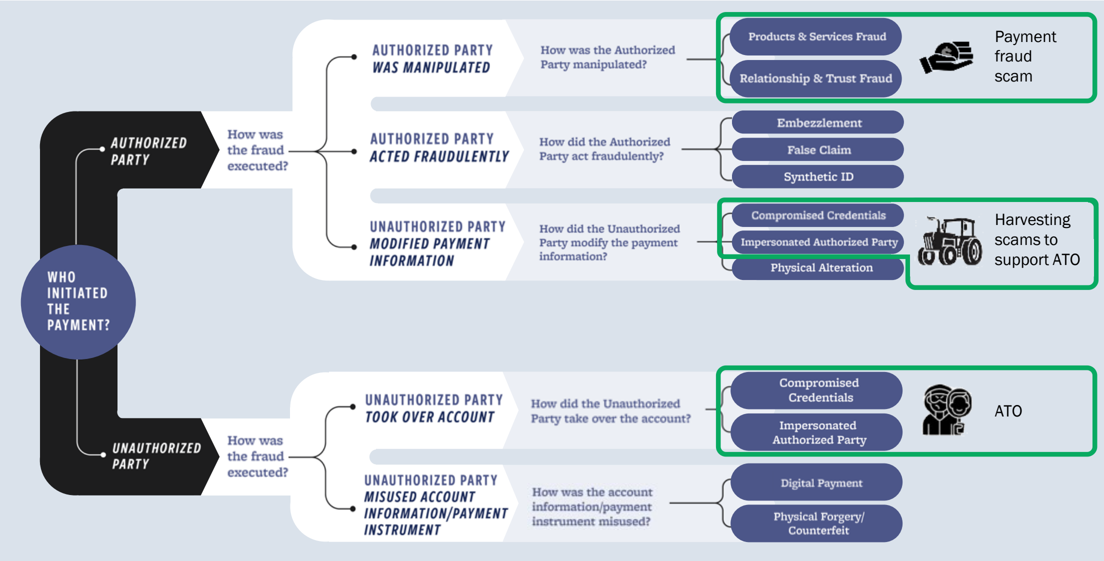
Source: U.K. Finance

In contrast to the U.K., FIs in North America have relatively few consistent standards for defining terms and characteristics. What taxonomies exist are either stuck in perpetual disputes or are in the earliest stages of adoption and tend to err on the side of conceptual guide vs. functional specification. The American Banking Association (ABA) has developed a relatively simple taxonomy and some high-level definitions that it uses for benchmarking. Still, many fraud executives complain that there is little consistency in how each member interprets those definitions. One fraud executive comments that the ABA benchmarks are "helpful in the abstract" but that significant variation in how contributors interpret the definitions "leads to questions about how accurately the benchmarks reflect what's actually going on."

The Federal Reserve's FedPayments Improvement program developed and deployed the Fraud Classifier Model in 2020.[2] The Fraud Classifier Model is useful as a conceptual model for a top-down taxonomy and as a guide for classifying fraud at a very high level. For example, it does well to demonstrate how the difference between scams and ATO comes down to whether the fraudster seeks to deceive the legitimate owner (or their authorized agent) into issuing instructions or whether they seek to deceive the institution into believing that the instructions are issued by the legitimate owner (or authorized agent). It is a helpful guide, but it stops short of providing a structure that bridges the gap between a high-level, top-down categorization and a set of standard definitions of fraud categories, types, and subtypes that FIs could use as specifications for reporting fraud consistently. Ideally, the Fraud Classifier could be a foundational guide for developing a more detailed collection of fraud categories (Figure 2).

[2] "FraudClassifier Model," The Federal Reserve's FedPayments Improvement Program, accessed November 18, 2021, https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/.

FIGURE 2: THE FEDERAL RESERVE'S FRAUD CLASSIFIER MODEL


WHO INITIATED THE PAYMENT?
AUTHORIZED PARTY
How was the fraud executed?
AUTHORIZED PARTY WAS MANIPULATED
How was the Authorized Party manipulated?
Products & Services Fraud
Relationship & Trust Fraud
Payment fraud scam
AUTHORIZED PARTY ACTED FRAUDULENTLY
How did the Authorized Party act fraudulently?
Embezzlement
False Claim
Synthetic ID
UNAUTHORIZED PARTY MODIFIED PAYMENT INFORMATION
How did the Unauthorized Party modify the payment information?
Compromised Credentials
Impersonated Authorized Party
Physical Alteration
Harvesting scams to support ATO
UNAUTHORIZED PARTY
How was the fraud executed?
UNAUTHORIZED PARTY TOOK OVER ACCOUNT
How did the Unauthorized Party take over the account?
Compromised Credentials
Impersonated Authorized Party
ATO
UNAUTHORIZED PARTY MISUSED ACCOUNT INFORMATION/PAYMENT INSTRUMENT
How was the account information/payment instrument misused?
Digital Payment
Physical Forgery/ Counterfeit

Source: Federal Reserve Bank of Boston

Such a taxonomical structure could allow for fraud types and sub-types to be subordinated under fraud categories, and in such a way that is compatible with the U.K. taxonomy. This would open the door for FIs to collaborate on creating more specific and standard definitions for terms and develop reporting specifications that would enable industrywide benchmarking. If it aligned with elements of U.K. Finance's taxonomy, then it could even be used as means of international benchmarking for the types of fraud that share a common framework.

Neither approach to categorizing scams has made an important step to help draw clearer distinctions between forensic patterns of attack and the methods used to commission the theft. Namely, neither categorizes the types of scams intended to harvest sensitive information from the victim separately from the types of scams intended to deceive the victim into initiating a fraudulent payment.[3] Such a classification method would distinguish scam activities that enable fraud (often adjacent types of fraud that occur downstream, e.g., ATO) from the types of scam activities that are directly tied to a fraud attack. Table B illustrates the difference between "harvesting scams" and "payment fraud scams."

[3] See Aite-Novarica Group's report Trends in Fraud in the Digital Channel: Fraud Inc. Pivoting to Scams, December 2021.

TABLE B: CLASSIFYING SCAMS BY THEIR OBJECTIVE

SCAM CLASS	DESCRIPTION OF THEIR OBJECTIVE
Harvesting scams	These scams are primarily designed to deceive the victim into revealing sensitive information to support fraud attacks that may occur later or at another institution.
Payment fraud scams	These scams are primarily designed to deceive or coerce the victim into making a fraudulent payment.

Source: Aite-Novarica Group

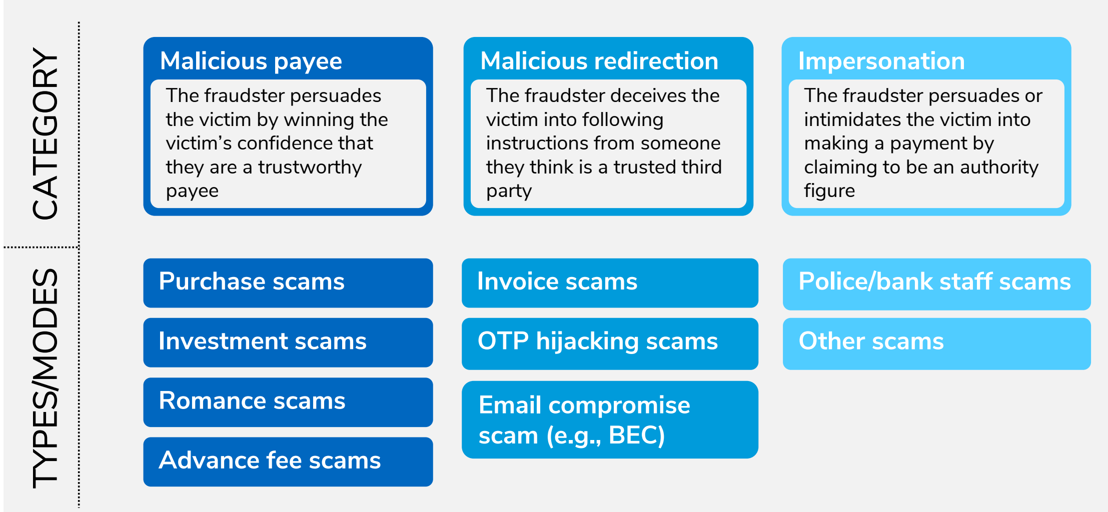
Distinguishing between these would help improve the accuracy of reporting on scam activity and reveal insights into the effectiveness of countermeasures. Classifying by the objective of the scam is also helpful for distinguishing between subordinate types of scams.

Fraudsters have specialized their attack patterns according to the objective of their attacks; their forensic attack patterns are often unique to the objective of the scam. Investing in an awareness campaign that specifically targets reducing the effectiveness of phishing attacks, for example, is unlikely to reduce scam claims but may reduce ATO losses. Conversely, investing in orchestrating behavioral biometric signal detection with a transaction monitoring fraud detection solution may pay dividends in reducing scam claims but will not reduce phishing attacks.

Categorizing, Conceptualizing, and Defining Scams

In categorizing scams, it's helpful to leverage the lessons learned from U.K. Finance's fraud taxonomy. Its taxonomy breaks scams down into scam categories and scam types or modes of attack. Scam categories align with the methods that fraudsters use to deceive the victim (e.g., posing as a trustworthy payee, duping the victim into believing that they are an authority figure), and the scam types are specific patterns of attack that are commonly used examples of those methods. Figure 3 leverages such a structure to illustrate how specific types of payment fraud scams might break down hierarchically under a structure similar to U.K. Finance's taxonomy.

FIGURE 3: CONCEPTUAL PAYMENT SCAM TAXONOMICAL STRUCTURE



CATEGORY

TYPES/MODES

Malicious payee

The fraudster persuades the victim by winning the victim's confidence that they are a trustworthy payee

Malicious redirection

The fraudster deceives the victim into following instructions from someone they think is a trusted third party

Impersonation

The fraudster persuades or intimidates the victim into making a payment by claiming to be an authority figure

Purchase scams

Investment scams

Romance scams

Advance fee scams

Invoice scams

OTP hijacking scams

Email compromise scam (e.g., BEC)

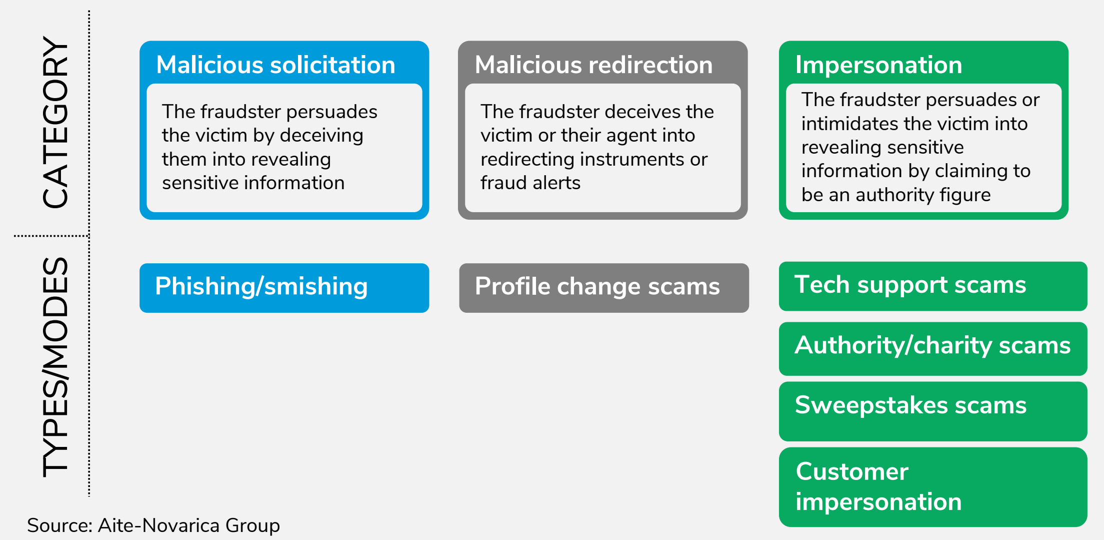
Police/bank staff scams

Other scams

Source: Aite-Novarica Group

A similar structure could conceivably apply to harvesting scams, as Figure 4 illustrates.

FIGURE 4: CONCEPTUAL HARVESTING SCAM TAXONOMICAL STRUCTURE



CATEGORY

TYPES/MODES

Malicious solicitation

The fraudster persuades the victim by deceiving them into revealing sensitive information

Malicious redirection

The fraudster deceives the victim or their agent into redirecting instruments or fraud alerts

Impersonation

The fraudster persuades or intimidates the victim into revealing sensitive information by claiming to be an authority figure

Phishing/smishing

Profile change scams

Tech support scams

Authority/charity scams

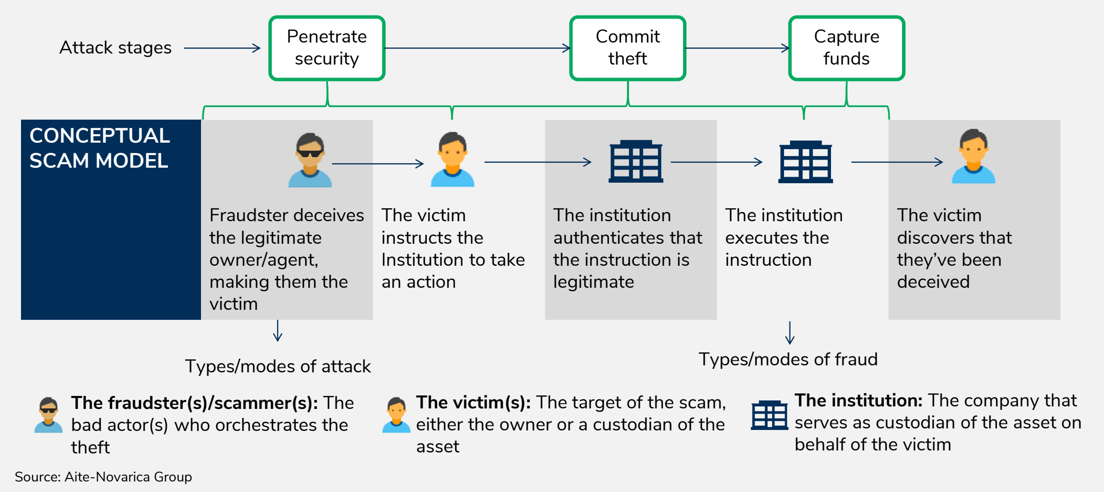
Sweepstakes scams

Customer impersonation

Source: Aite-Novarica Group

In deconstructing how a typical scam unfolds, consider the model in Figure 5. The fraudster must first penetrate the victim's security by using one of the types (or modes) of payment scam attack patterns. Once the fraudster has successfully deceived the victim, they commit the theft by manipulating the victim to issue payment instructions to their FI. Finally, the fraudster or one of their confederates captures the stolen funds and moves them to an account safe from recovery efforts or converts them to cash.

FIGURE 5: PAYMENT SCAM CONCEPTUAL MODEL


Attack stages
Penetrate security
Commit theft
Capture funds
CONCEPTUAL SCAM MODEL
Fraudster deceives the legitimate owner/agent, making them the victim
The victim instructs the Institution to take an action
The institution authenticates that the instruction is legitimate
The institution executes the instruction
The victim discovers that they've been deceived
Types/modes of attack
Types/modes of fraud
The fraudster(s)/scammer(s): The bad actor(s) who orchestrates the theft
The victim(s): The target of the scam, either the owner or a custodian of the asset
The institution: The company that serves as custodian of the asset on behalf of the victim

Source: Aite-Novarica Group

Such a model allows the practitioner to record the mode of attack and the type of fraud. In doing so, the FI can quantify the frequency and severity of the forensic attack patterns that fraudsters prefer in addition to the modes of theft they prefer. Quantifying both reveals the vulnerabilities that the FI would need to remediate to bolster defenses and enables the FI to measure whether and to what degree remediation efforts positively or negatively impact attacks and losses.

The means of categorizing the types/modes of fraud have been established according to accounting practices that most FIs adhere to for charging off losses (often according to the type of payment service or business unit that manages the core payment function that the fraudster used). However, the means of categorizing the modes of types/modes of attack in markets outside the U.K. are still largely without consistent form and function.

Figure 3 and Figure 4 illustrate the hierarchical structure that aligns well with U.K. Finance's model. Table C and Table D describe the types/modes of attack that align with U.K. Finance's taxonomy.

TABLE C: PAYMENT FRAUD SCAM ATTACK TYPE DESCRIPTIONS

SCAM CLASS	ATTACK TYPE	DESCRIPTION
Malicious payee	Purchase scam	The victim pays in advance for goods or services they never receive. These scams usually involve the victim using an online platform, such as an auction website or social media. They are commonly observed in person-to-person (P2P) payments such as Zelle, PayPal, and Venmo.
	Investment scam	A criminal convinces their victim to move money to a fictitious fund or pay for a fake investment. These scams should not be confused with scams leading to ATO attempts to cash out investment/retirement accounts.
	Romance scam	The victim is persuaded to pay a person they have met, often online through social media or dating websites, and with whom they believe they are in a relationship.
	Advance fee scam	The fraudster convinces the victim to pay a fee that they claim will release a much larger payment or high-value goods.
Malicious redirection	Invoice scam	The fraudster convinces the victim to pay or redirect a payment for an invoice to an account the fraudster controls. Commonly observed among treasury and payments clients, this type is gaining momentum among consumers in some markets, such as the U.K.
	OTP hijacking scams	The fraudster seeks to deceive the victim into revealing the OTP that the victim's FI sent them for the purpose of releasing a fraudulent payment.
	Email compromise scam	The fraudster takes control of a trusted third party's email system (or cleverly disguises an email to appear to come from a trusted source) to instruct the victim to send payment to a fraudster's account. It appears most commonly as BEC or email account compromise (EAC). It disproportionately affects treasury clients, but it also has a consumer variant that often targets consumer real estate transactions.

SCAM CLASS	ATTACK TYPE	DESCRIPTION
Impersonation	Bank staff scam	The fraudster contacts the victim purporting to be from their bank and convinces them to make a payment to an account the fraudster controls. This scam should not be confused with one-time passcode (OTP) scams, which lead to victims revealing bank-issued multifactor authentication (MFA) codes to release a payment.
	Other impersonation scam	The fraudster claims to represent an organization such as a utility company, tech support, close friend or family member, or a government agency and convinces the victim to make a payment. This scam should not be confused with tech support scams that lead victims to reveal personally identifiable information (PII) or credentials used for an ATO attack.

Source: Aite-Novarica Group

TABLE D: HARVESTING SCAM ATTACK TYPE DESCRIPTIONS

SCAM CLASS	ATTACK TYPE	DESCRIPTION
Malicious solicitation	Phishing/smishing	This is the most common form of automated attack. The fraudster uses links in email or SMS messages to direct the victim to a site designed to capture sensitive information.
Malicious redirection	Profile change scams	The fraudster uses social engineering techniques to deceive an agent (usually from the FI's contact center) into changing the victim's profile information or redirecting the delivery of a payment instrument or security alerts.

SCAM CLASS	ATTACK TYPE	DESCRIPTION
Impersonation	Tech support scams	The fraudster impersonates a trusted organization's tech support agent and convinces the victim to turn over control of their device to the fraudster or follow a set of instructions that leads to capturing sensitive information.
	Authority/charity scams	The fraudster claims to represent an organization such as a utility company, charity, close friend or family member, or a government agency and convinces the victim to reveal sensitive information.
	Sweepstakes scams	The victim is deceived into revealing sensitive information to qualify for a bogus windfall.
	Customer impersonation	The fraudster impersonates the victim and deceives the FI's agent into revealing sensitive information about the victim.

Source: Aite-Novarica Group

ESTIMATING THE MAGNITUDE OF SCAM ACTIVITY

A variety of ways can measure the scale of scam activity and the rate of its growth. However, most measures of scam activity are restricted to segments of discrete markets, specific patterns of attack, or the peculiarities of the institutions or government agencies that are taking the measurements.

According to its annual report on fraud losses, U.K. Finance revealed that authorized push payment (APP) fraud losses grew 5% or from 455.8 million pounds to 479.0 million pounds between 2019 and 2020 in the U.K. market. In a report released in H2 2021, it revealed that "APP fraud losses increased 71% during the first half of 2021—surpassing the amount of money stolen through card fraud for the first time."[4] Katy Worobec, Managing Director of Economic Crime at U.K. Finance, summarized the threat in its annual report by saying, "The links between fraud, organized crime, and terrorism pose a significant and growing threat to our national security."[5]

The U.K.'s measurements are clear, precise, and insightful, and they are specific to the kinds of scams that affect FIs. Measuring the scale and rate of growth in scam activity in the other markets is more difficult. For example, the U.S. Federal Trade Commission (FTC) collects and reports on a wide variety of scam activities. Its data come from federal and state law enforcement agencies and include an exceptionally broad array of criminal activities that are often poorly defined and intermixed to the point that it becomes difficult to tease out the kinds of scams that impact FIs and their customers from those that impact the broader population. However, it provides reporting on specific forms of scams that are predominantly oriented around FIs and their customers.

Specifically, in February 2021, the FTC released a bulletin that revealed that "the amount consumers reported losing to romance scammers is up about 50% since 2019 and has increased more than fourfold since 2016."[6] In a similar bulletin from February 2021, the FTC revealed that overall scam activity in the U.S., including scams that affect consumers, grew from US$1.8 billion in losses in 2019 to US$3.3 billion in losses in 2020.

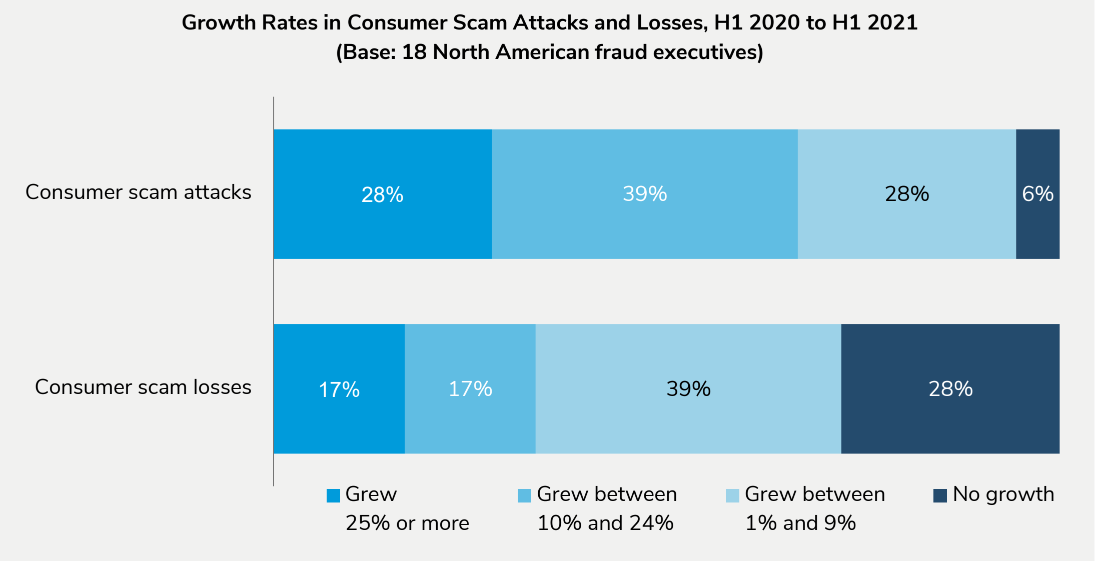
The one thing that all of these observations share is a noteworthy growth rate. North American fraud executives also observed this rate of growth (Figure 6).

[4] "2021 Half Year Fraud Update", U.K. Finance, September 2021, accessed January 31, 2022, https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2021-FINAL.pdf.

[5] "Fraud—The Facts 2021," U.K. Finance, March 25, 2021, accessed January 31, 2022, https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2021.

[6] "New FTC Data Show Massive Increase in Romance Scams, $304M in Losses," Federal Trade Commission, February 10, 2021, accessed January 31, 2022, https://www.ftc.gov/news-events/press-releases/2021/02/new-ftc-data-show-massive-increase-romance-scams-304m-losses.

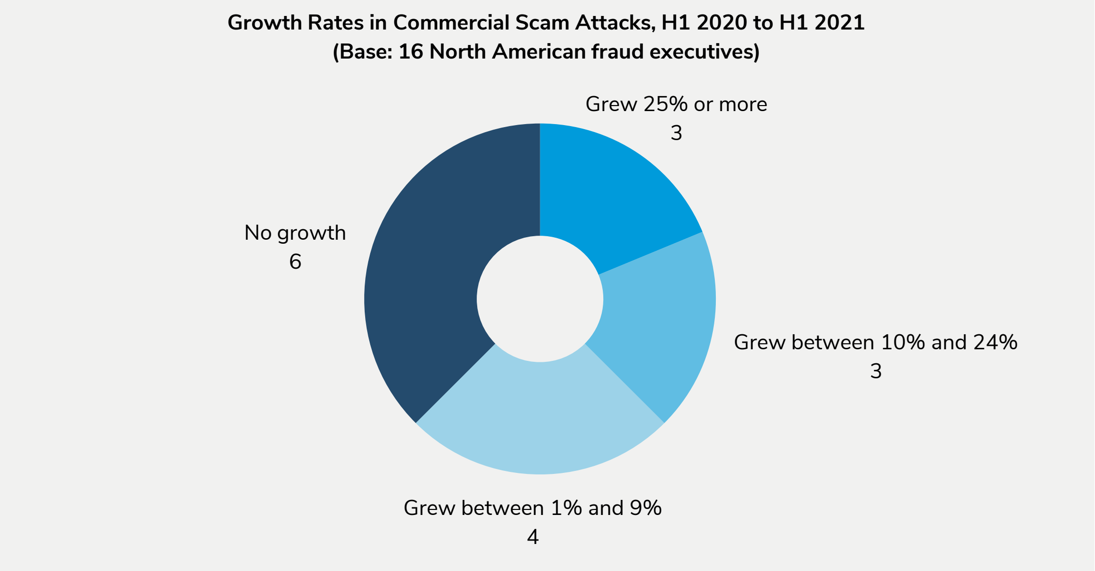
FIGURE 6: GROWTH RATES IN CONSUMER SCAM ATTACKS AND LOSSES



Source: Aite-Novarica Group survey of 18 North American fraud executives, October 2021

The increase in scam activity targeting commercial customers is not as widely distributed as those impacting consumers. Still, it remains noteworthy because, as many fraud executives point out, it's been growing steadily for the last several years, driven primarily by rising instances of BEC and EAC (Figure 7).

FIGURE 7: GROWTH RATES IN COMMERCIAL SCAM ATTACKS

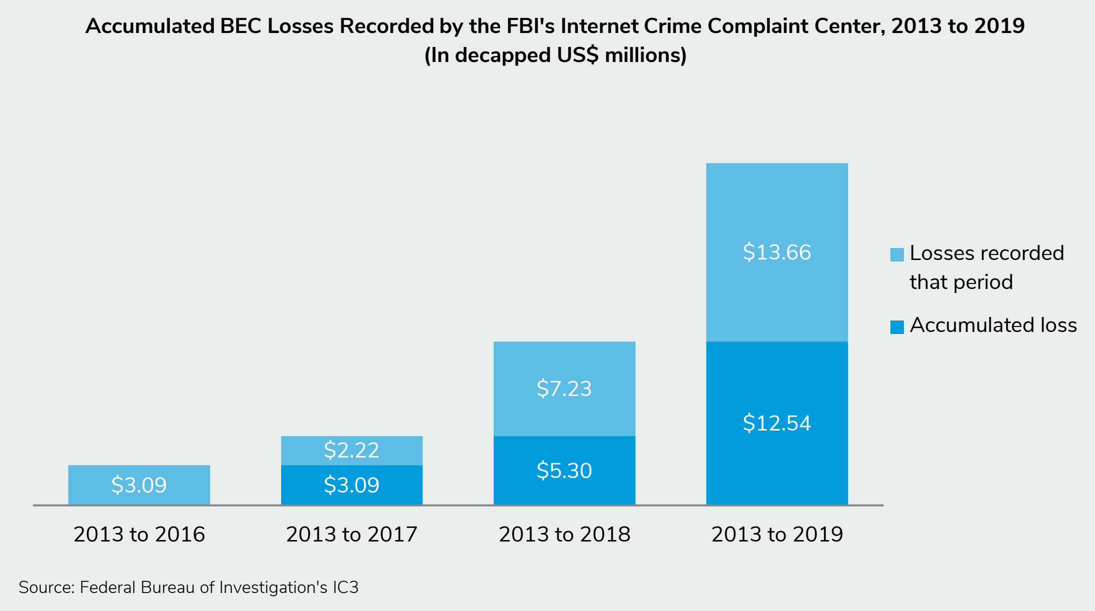


Source: Aite-Novarica Group survey of 18 North American fraud executives, October 2021

Corporate customers do not enjoy the same regulatory protections that consumers do when it comes to reimbursement for scams. As a result, few FIs reimburse corporate customers victimized by scam attacks. One result is that most FIs do not track the dollar amounts of losses their customers incur.

In the U.S., most FIs encourage corporate customers who have been victimized by a scam to notify law enforcement and register a complaint with the FBI’s Internet Crime Complaint Center (IC3). As a result, the IC3 tracks scam complaints, though its reporting is released somewhat inconsistently in terms of frequency. Between 2013 and 2019, however, IC3 released public-service bulletins on a relatively consistent basis and provided a running tally of BEC losses. Most fraud executives that Aite-Novarica Group interviewed believe that IC3’s reported figure is roughly one-third the size of actual losses (Figure 8).

FIGURE 8: RATE OF BEC GROWTH FROM 2013 TO 2019



Source: Federal Bureau of Investigation's IC3

Unfortunately, more recent bulletins IC3 has posted related to BEC and scams in general have not conformed to the same format as those it posted between 2013 and 2019. Despite this inconsistency, they have released some insights that reveal that scam complaints have continued trending upward.

In May 2021, IC3 released a bulletin announcing a grim milestone: It had collected more than 6 million complaints in the 21 years since its inception in March 2000. The bulletin revealed that complaints increased nearly 70% between 2019 and 2020. The most common complaints include phishing scams, nonpayment/nondelivery scams, and extortion, but those that resulted in the most significant amounts of loss included BEC, romance scams, and investment scams.[7]

DRIVING FORCES BEHIND THE INCREASE IN SCAM ACTIVITY

Fraud is an industry, and scams are one of several ways it generates revenue. Over the past decade, the fraud industry has benefitted handsomely from the disruption in card fraud caused by the EMV chip rollout.[8] In this regard, scams are like application fraud, ATO, and mule activity insofar as they are all derivative forms of the pervasive and

[7] "IC3 Logs 6 Million Complaints," Internet Crime Complaint Center, May 14, 2021, accessed January 31, 2022, https://www.fbi.gov/news/stories/ic3-logs-6-million-complaints-051721.

[8] See Aite-Novarica Group's report Key Trends Driving Fraud Transformation in 2021 and Beyond, December 2020.

endlessly expanding market for compromised and synthetic identities. As the supply of compromised and synthetic identities increases, they become more accessible, and the costs and barriers that prevent putting them to use subsequently diminish. In this regard, the increase in scam activity is driven by the market forces driving growth in fraud more broadly.

There are two other driving forces worth considering. They are recurring themes in observations that fraud executives have made on the nature and origins of increases in scam activity. Both align well with the broader market forces behind fraud in general:

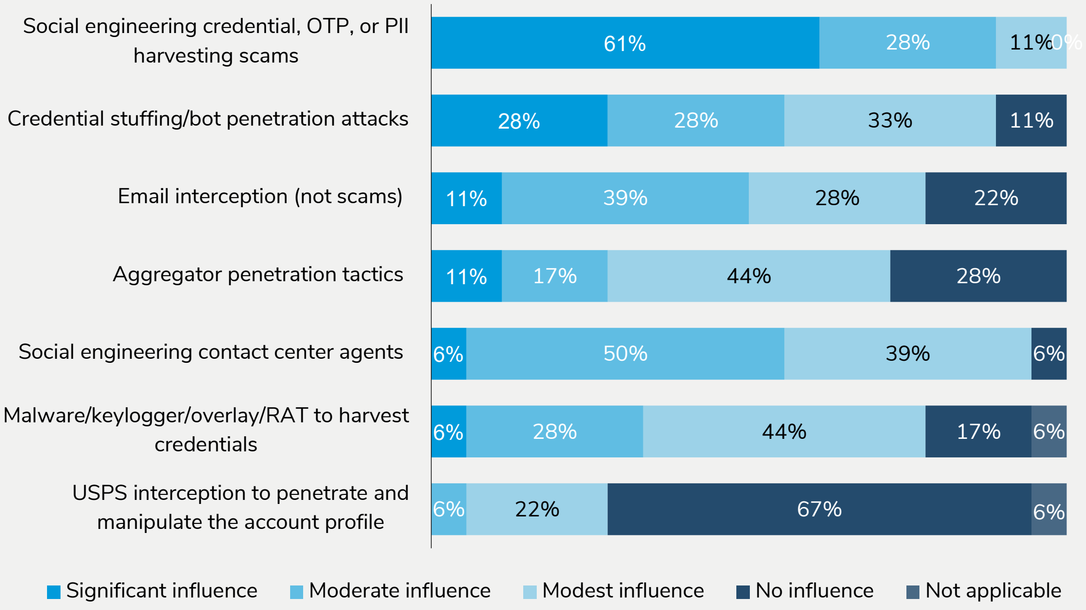
- The first has to do with the proliferation of digital-first banking and faster payments. These developments were a factor that increased scam activity in the U.K. A great deal of scam activity targets some of the faster payment networks in the U.S., but the jury is still out as to the degree to which it is driving scams in that market.[9]
- The second is a bit more abstract. Widespread investment in innovative and effective layers of authentication controls has made it costlier and more technically challenging for fraudsters to defeat the FI's controls. These conditions have driven fraudsters to less technically demanding modes of attack that emphasize targeting the customer's lack of security hygiene rather than attempt to defeat the more formidable defenses FIs deploy.

A closer examination of the attack patterns that fraudsters use reveals that modes of attack that require less technical proficiency are more widely distributed than those that require greater technical proficiency. Figure 9 illustrates the degree to which various penetration attack patterns (i.e., the methods that fraudsters use to deceive the victim or defeat fraud controls protecting the victim's account) influence digital fraud attack volume at FIs.

[9] See Aite-Novarica Group's report Market Trends in Mitigating Fraud Risk Related to Real-Time Payments, July 2020.

FIGURE 9: TRENDS IN PENETRATION ATTACK PATTERNS

Q. How would you estimate the rank of the following penetration tactics in terms of the relative degree to which it influences consumer digital attack volume at your FI? (Base: 18 North American fraud executives)



Source: Aite-Novarica Group survey of 18 North American fraud executives, October 2021

The high degree of influence social engineering has on digital fraud attack volume is particularly noteworthy. Social engineering attacks require very little technical proficiency. In contrast, every other form of attack requires some degree of technical training or automated assistance in the form of software to automate, obfuscate, or otherwise assist the attacker. Credential stuffing kits sold on dark web marketplaces not only are common but also have become remarkably sophisticated and easy for first-time would-be fraudsters to use. Still, methods of deception such as social engineering are easy for beginners to adopt and are highly effective. They are also often used in harvesting scams and payment fraud scams.

Social engineering's appeal to beginner fraudsters is notable given the pandemic's impact on fraud in general and scams in particular. Many fraud executives believe that the pandemic created a new and generously proportioned cohort of citizen fraudsters drawn into seeking income from stimulus fraud through a combination of conditions, including dire economic circumstances.[10] This trend implies that as pandemic stimulus programs terminate or come under more rigorous fraud controls, many of these newly minted citizen fraudsters are unlikely to return to legitimate sources of income on a full-time basis.

[10] See Aite-Novarica Group's report Market Trends in Fraud for 2022 and Beyond: New Fraudsters, New Era, February 2022.

CONSIDERING THE IMPLICATIONS OF MANAGING SCAMS

If the root cause of the increase in scam activity is somewhat academic to fraud executives, its implications certainly are not. Many fraud executives in North America point to the changes the U.K. market recently rolled out to address deteriorating public sentiment and increasing scrutiny from regulators and legislators as examples of the kinds of outcomes they may have to contend with if the rates of increase in scam activity follow a similar trajectory. Among those changes are the following programs that have been rolled out for many U.K. banks and building societies:

- **Confirmation of Payee:** A program for U.K.-based payments launched by Pay.UK in 2020. The program enables FIs to match the name of payment beneficiaries against the titles of the beneficiary accounts. In the event of a mismatch, the sending bank can prompt the customer of the mismatch, alerting them that their payment may not be going to the intended recipient. The U.K.'s payments regulator, the Payment Systems Regulator (PSR), has directed banks and building societies to implement the program. As of January 2022, more than 30 banks, building societies, and payment service providers (PSPs) offer the service to their customers.
- **Contingency Reimbursement Model:** The Contingency Reimbursement Model is a program devised by the PSR, organized by U.K. Finance, and overseen primarily by the Lending Standards Board (LSB) and the PSR and the Financial Conduct Authority (FCA). Participant volunteers know it as "the Code," and one fraud executive described it as "the least voluntary 'voluntary program.'" Its objective is "to reduce both the occurrence and impact of APP scams and is designed to give people the confidence that, if they fall victim to an APP scam and have acted appropriately, they will be reimbursed."[11] The program does this through a set of standards meant to create a consistent process for resolving scam claims.

These programs came about in response to a "super complaint" filed by Which, a leading consumer advocacy group in the U.K. Which brought the matter to the attention of the FCA, and it later came to the attention of the PSR, the LSB, and Parliament. Which filed the super complaint in 2016 in response to a rising tide of complaints from bank customers frustrated by being denied reimbursement for APP scams. The super complaint triggered the commissioning of a Parliamentary report on economic crime,

[11] "APP Scams," Payment Systems Regulator, November 2021, accessed February 2022, https://www.psr.org.uk/our-work/app-scams/.

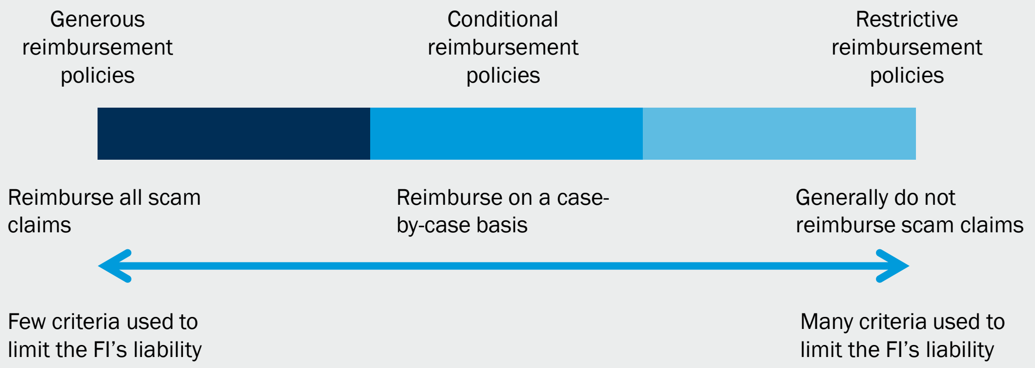
published in October 2019. The report included several recommendations, including a 24-hour delay on all first-time payments to new payees and what ultimately became Confirmation of Payee (also referred to as Payee Name Verification) and the Contingency Reimbursement Model. The recommendation to slow down real-time payments for first-time payees never became policy, but it illustrated to U.K. bankers how significant a problem legislators and treasury officials considered the conditions of APP fraud to be.

As scam activity increases in other markets, fraud executives have become particularly attentive to signals from regulators and consumer advocacy groups that they may be considering taking similar actions. This has been of particular concern to many FIs because of the profoundly negative impact that scams have on the client experience—and because many fraud executives lack confidence in their capacity to mitigate the risks. FIs in the U.S. market are also concerned because of inconsistencies between their reimbursement policies and how regulators such as the CFPB have signaled their intentions to enforce the provisions of Regulation E (Reg E), which govern scenarios for reimbursement among some claims that are the downstream result of harvesting scams.

SIGNS OF CHANGE IN REIMBURSEMENT POLICIES IN THE U.S.

In June and December 2021, the CFPB issued FAQ bulletins to clarify its interpretation of several sections of the Electronic Fund Transfer Act (EFTA) and Reg E. Of particular importance to fraud executives were the bureau's answers to questions under the "Error Resolution: Unauthorized EFTs" section. This section is meant to illustrate the bureau's perspective on a collection of scenarios that some FIs factor into their reimbursement policies as criteria for limiting or restricting liability for some claims. There is a good deal of inconsistency in reimbursement policies among FIs in the U.S. One way to measure the differences in reimbursement policies is by the extent to which they use criteria to limit liability for reimbursement for what a customer claims to be unauthorized payments. Figure 10 illustrates a conceptual spectrum to visualize the different approaches FIs take when shaping their reimbursement policies.

FIGURE 10: CONCEPTUAL MODEL OF THE SPECTRUM OF CONSUMER REIMBURSEMENT POLICIES


Generous reimbursement policies
Conditional reimbursement policies
Restrictive reimbursement policies
Reimburse all scam claims
Reimburse on a case-by-case basis
Generally do not reimburse scam claims
Few criteria used to limit the FI's liability
Many criteria used to limit the FI's liability

Source: Aite-Novarica Group

Most FIs structure their reimbursement policies around various conditional criteria that they use to determine the degree to which the claim justifies reimbursement. On the generous end of the spectrum, the criteria used to determine the FI's liability for reimbursement tend to be designed to expose abusive claims made by individuals who demonstrate evidence that they were colluding with the alleged attackers, for example. An FI on the opposite end of the spectrum is likely to have many more criteria for disqualifying claims based on evidence of collusion, along with several additional criteria. These criteria are designed to exempt the FI from reimbursing claims that they believe to be frivolous or the result of gross negligence on behalf of the consumer's efforts to safeguard their account from unauthorized access.

Table E provides a sample of the kinds of criteria observed by the CFPB (illustrated in the form of a frequently asked question) that most FIs use to determine liability for reimbursing claims of ATO that are often the downstream result of harvesting scams. It also includes the bureau's perspective on whether FIs can use these to determine liability according to the EFTA and Reg E.

TABLE E: CFPB GUIDANCE ON CRITERIA FOR DETERMINING LIABILITY FOR REIMBURSEMENT

QUESTION/SCENARIO/CRITERIA	CFPB'S RESPONSE
Question 3: Is an EFT from a consumer's account initiated by a fraudster through a nonbank P2P payment provider considered an unauthorized EFT?	Yes. Because the EFT was initiated by a person other than the consumer without actual authority to initiate the transfer—i.e., the fraudster—and the consumer received no benefit from the transfer, the EFT is an unauthorized EFT. 12 CFR 1005.2(m). This is true even if the consumer does not have a relationship with, or does not recognize, the nonbank P2P payment provider.
Question 4: Does an EFT initiated by a fraudster using stolen credentials meet the Regulation E definition of an unauthorized EFT?	Yes. As discussed in Electronic Fund Transfers Error Resolution: Unauthorized EFT Question 1, Regulation E defines an unauthorized EFT as a transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit. 12 CFR 1005.2(m). When a consumer's account access information is obtained from a third party through fraudulent means, such as computer hacking, and a hacker uses that information to make an EFT from the consumer's account, the transfer is an unauthorized EFT under Regulation E. For example, the bureau is aware of the following situations involving unauthorized EFTs: • A consumer shares their account access information in order to enter into a transaction with a third party, such as a merchant, lender, or employer offering direct deposit, and a fraudster obtains the consumer's account access information by hacking into the computer system of the third party. The fraudster then uses a bank-provided P2P payment application to initiate a credit push payment out of the consumer's deposit account. • A consumer shares their debit card information with a P2P payment provider in order to use a mobile wallet. A fraudster then hacks into the consumer's phone and uses the mobile wallet to initiate a debit card transfer out of the consumer's deposit or prepaid account. • A thief steals a consumer's physical wallet and initiates a payment using the consumer's stolen debit card. • See Electronic Fund Transfers Error Resolution: Unauthorized EFTs Question 5 for more examples of unauthorized EFTs.

QUESTION/SCENARIO/CRITERIA	CFPB'S RESPONSE
	All of the FIs in these examples, including any nonbank P2P payment provider or deposit account-holding FI, must comply with the error resolution requirements discussed in Electronic Fund Transfers Error Resolution Question 2, as well as the liability protections for unauthorized transfers in 12 CFR 1005.6.
Question 5: A third party fraudulently induces a consumer into sharing account access information that is used to initiate an EFT from the consumer's account. Does the transfer meet Regulation E's definition of an unauthorized EFT?	Yes. As discussed in Electronic Fund Transfers Error Resolution: Unauthorized Fund Transfers Question 1, Regulation E defines an unauthorized EFT as an EFT from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit. 12 CFR 1005.2(m). Comment 1005.2(m)-3 explains further that an unauthorized EFT includes a transfer initiated by a person who obtained the access device from the consumer through fraud or robbery. Similarly, when a consumer is fraudulently induced into sharing account access information with a third party, and a third party uses that information to make an EFT from the consumer's account, the transfer is an unauthorized EFT under Regulation E. For example, the bureau is aware of the following situations in which a third party has fraudulently obtained a consumer's account access information, and thus, are considered unauthorized EFTs under Regulation E: (1) a third party calling the consumer and pretending to be a representative from the consumer's FI and then tricking the consumer into providing their account login information, texted account confirmation code, debit card number, or other information that could be used to initiate an EFT out of the consumer's account, and (2) a third party using phishing or other methods to gain access to a consumer's computer and observe the consumer entering account login information. EFTs stemming from these situations meet the Regulation E definition of unauthorized EFTs.

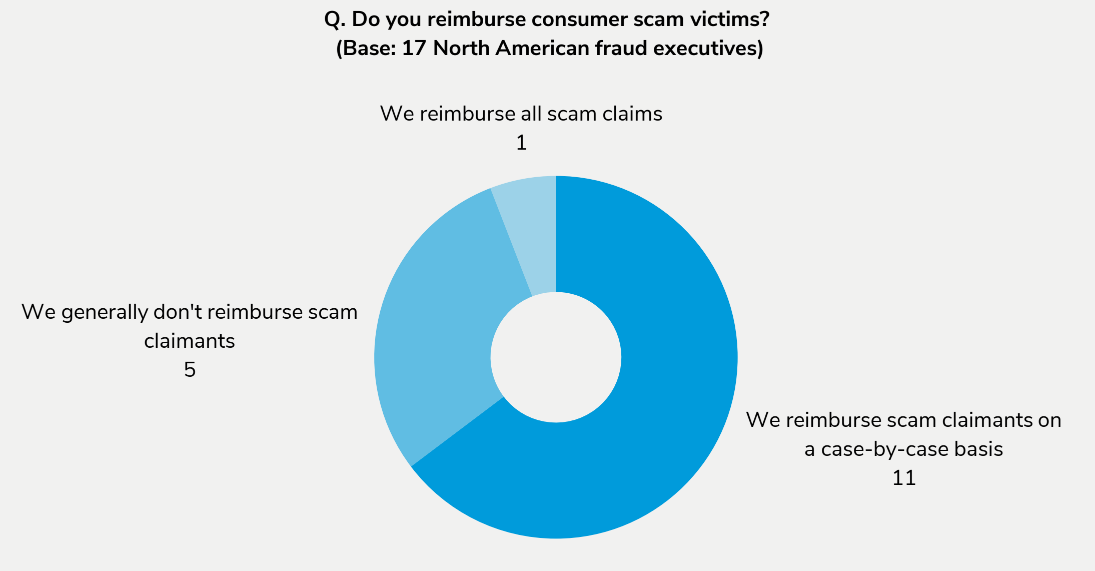
QUESTION/SCENARIO/CRITERIA	CFPB'S RESPONSE
Question 6: If a third party fraudulently induces a consumer to share account access information, are subsequent transfers initiated with the fraudulently obtained account information excluded from Regulation E's definition of unauthorized electronic funds transfer because they are initiated "by a person who was furnished access device to the consumer's account by the consumer"?	No. A consumer who is fraudulently induced into providing account information has not furnished an access device under Regulation E. As explained above in Electronic Fund Transfers Error Resolution: Unauthorized EFTs 3, 4, and 5, EFTs initiated using account access information obtained through fraud or robbery fall within the Regulation E definition of unauthorized EFT. See Comment 1005.2(m)-3.
Question 7: Can an FI consider a consumer's negligence when determining liability for unauthorized EFTs under Reg E?	No. Regulation E sets forth the conditions in which consumers may be held liable for unauthorized transfers, and its commentary expressly states that negligence by the consumer cannot be used as the basis for imposing greater liability than is permissible under Regulation E. 12 CFR 1005.6; Comment 6(b)-2. For example, consumer behavior that may constitute negligence under state law, such as situations when the consumer wrote the PIN on a debit card or on a piece of paper kept with the card, does not affect the consumer's liability for unauthorized transfers under Regulation E. Comment 1005.6(b)-2.

QUESTION/SCENARIO/CRITERIA	CFPB'S RESPONSE
Question 9: If an FI's agreement with a consumer includes a provision that modifies or waives certain protections granted under Regulation E, such as waiving Regulation E liability protections if a consumer has shared account information with a third party, can the institution rely on its agreement when determining whether the EFT was unauthorized and whether related liability protections apply?	No. EFTA includes an anti-waiver provision stating that "[n]o writing or other agreement between a consumer and any other person may contain any provision that constitutes a waiver of any right conferred or cause of action created by [EFTA]." 15 U.S.C. § 1693l. Although there may be circumstances when a consumer has provided actual authority to a third party under Regulation E according to 12 CFR 1005.2(m), an agreement cannot restrict a consumer's rights beyond what is provided in the law, and any contract or agreement attempting to do so is a violation of EFTA.
Question 11: A fraudster initiates an EFT through a nonbank P2P payment provider that the consumer does not have a relationship with from the consumer's account with a depository institution. Is the depository institution considered an FI with full error resolution obligations under Regulation E?	Yes. As discussed in Electronic Fund Transfers Coverage: Financial Institutions Question 1, the definition of "financial institution" includes a bank, savings association, credit union, or any other person that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide EFT services. 12 CFR 1005.2(i). Here, the account-holding FI holds the consumer's account and is thus considered an FI under Regulation E. Any entity defined as an FI under Regulation E has error resolution obligations in the event that a consumer notifies the FI of an error, with limited exceptions. 12 CFR 1005.11. As discussed in Electronic Fund Transfers Error Resolution: Unauthorized Transfers Question 4, since the transaction is an unauthorized EFT, the depository institution must comply with any applicable liability protections for unauthorized transfers in 12 CFR 1005.6.

Source: CFPB

The CFPB's guidance as articulated in these bulletins is noteworthy because it questions the basis of many of the conditional criteria baked into reimbursement policies specific to unauthorized payment claims among many FIs in the U.S. Reimbursement policies specific to claims of payment fraud scams (or authorized payment scams) skew decidedly in the direction of more restrictive criteria (Figure 11).

FIGURE 11: DISTRIBUTION OF CONSUMER SCAM REIMBURSEMENT POLICIES AMONG U.S. FIS



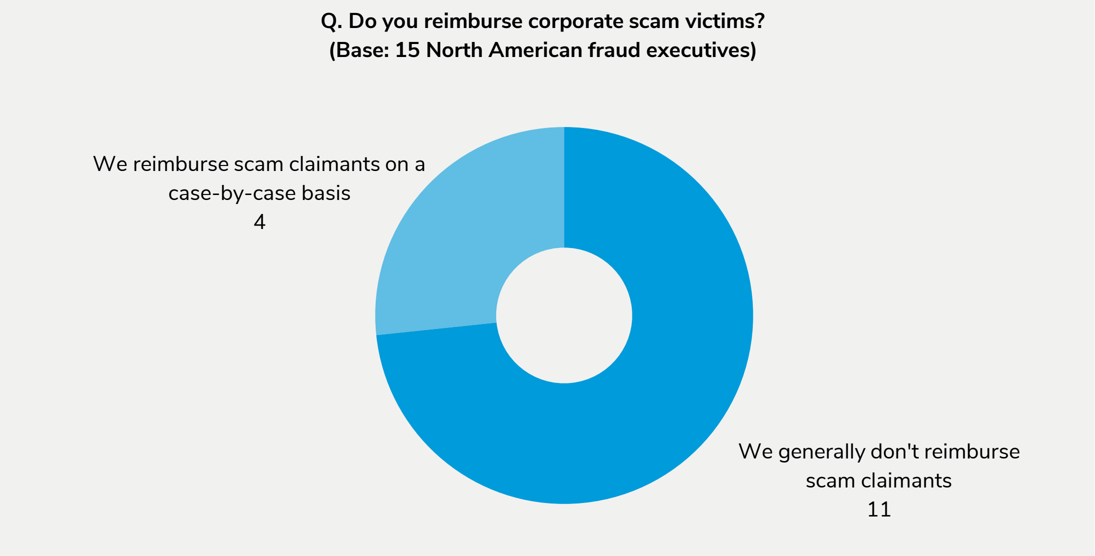
Source:Aite-Novarica Group survey of 18 North American fraud executives, October 2021

The implication of the CFPB's guidance is potentially significant, even if it is restricted to unauthorized payment claims. Many FIs with restrictive conditions for reimbursing unauthorized payment claims will need to make substantive changes to those policies or prepare to defend them. On the line will be millions of dollars in net-new losses incurred primarily by those FIs that have historically relied on one or more criteria used to determine liability that the CFPB now claims are illegitimate for denying claims for unauthorized payments that are often the result of harvesting scams. Also on the line could be many more millions of dollars in fines, litigation, remediation programs, and additional risk and compliance program costs necessary to defend or transform reimbursement policies. Most of these costs would be amplified by growth in harvesting scam activity.

Impact on Commercial Customers

Commercial customers don't enjoy the same degree of protection as consumers do regarding reimbursement policies. Many FIs do not track scam attacks among their commercial customers, much less the losses that their commercial customers suffer from these attacks. Some reimburse in circumstances where the FI could be found culpable for failing to enforce “commercially reasonable” fraud detection and security controls under the Uniform Commercial Code (UCC) or in circumstances where the loss threatens an otherwise profitable or high-profile relationship. However, most FIs fall squarely on the “restrictive criteria” end of the reimbursement policy spectrum for reimbursing claims of authorized payment fraud by their commercial customers (Figure 12).

FIGURE 12: DISTRIBUTION OF COMMERCIAL SCAM REIMBURSEMENT POLICIES AMONG U.S. FIS



Source: Aite-Novarica Group survey of 18 North American fraud executives, October 2021

Neither fraud executives nor their counterparts in commercial banking units need to be concerned about the potential for a shift in liability for reimbursements for the losses suffered by their commercial customers. Still, they are growing alarmed by the volume of negative client experiences reported by those customers. Given the rate of growth in BEC (Figure 8) and the alarming pace of growth in ransomware attacks, many fraud executives and commercial bankers are understandably eager to find ways to mitigate these risks and protect their customers from a truly horrendous customer experience.

MITIGATION STRATEGIES

Part of the reason scams are problematic for FIs has to do with how difficult they are to detect and prevent. By focusing their attack on deceiving the customer and convincing them either to reveal key elements of sensitive information or to send a payment to confederate beneficiaries, they can bypass most, if not all, of the FI's authentication controls. Fraud operations units then have to rely exclusively on transaction monitoring controls or on programs aimed at proactively arming their customers with an awareness of the threat in the hopes that a sense of heightened vigilance will be sufficient to prevent the attacker from successfully deceiving the victim. The consensus among most fraud executives is that these strategies may be necessary and somewhat helpful but are far from effective on their own.

There is a growing and as-of-yet unmet demand for more innovative solutions that are deliberately designed to provide more robust scam detection performance. While innovative technologically oriented solutions are, indeed, sorely needed, it's also important to acknowledge that the scale of the challenge is such that those solutions, while necessary, won't be sufficient. Solution providers and FIs need to emphasize collaboration among themselves and their customers, and with law enforcement, payment networks, telecommunications carriers, social media companies, regulators, and even legislators to improve the security of the ecosystem.

PROACTIVE PREVENTION STRATEGIES

Investment has been prioritized for ATO and application fraud controls due to the lack of liability for reimbursing payment scam victims. These investments pay attractive dividends from a security standpoint and a client experience perspective. Some fraud executives and many solution providers argue that investing in controlling for application fraud and ATO is a preventive means of controlling scams. The argument posits that controlling for application fraud improves an FI's ability to disrupt mule rings that fraud rings often use as the logistical backbone supporting fraud and scam attacks.[12] Similarly, controlling for ATO disrupts the downstream outcomes of harvesting scams.

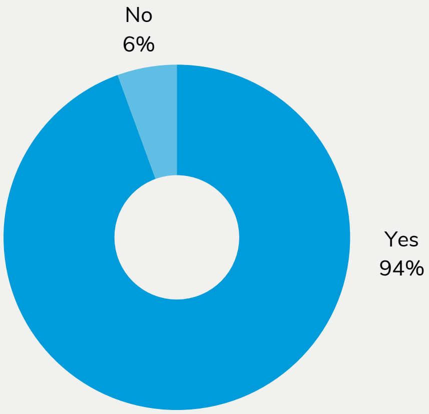
[12] See Aite-Novarica Group's report The Emerging Case for Proactive Mule Detection: Going on the Offense to Defend Reputational Risk, December 2021.

This argument has merit, and few question the client experience and security benefits of prioritizing investment in identity verification and authentication controls. Still, it is worth examining other prevention methods and how they've performed.

Historically, many fraud executives mention proactive security communication and awareness campaigns when asked what controls they have that are deliberately designed to combat scam activity. Many of these, of course, are oriented to address specific threats that tend to target discrete segments of their customers. If an FI's commercial customers, for example, are suffering from a spate of BEC attacks, the FI will likely launch an education and awareness campaign targeted at those customers to ensure they are aware of the threat, know what to watch out for, and know how to respond to an attack if it should happen to them. Many of these programs are campaign-oriented and, therefore, often transitory in nature. But 94% of FIs report having a proactive communications program that covers general security practices (Figure 13).

FIGURE 13: DISTRIBUTION OF PROACTIVE COMMUNICATION AND AWARENESS PROGRAMS

Q. Does your FI have a formal program for proactively communicating with your clients about how to maintain and improve security practices?
(Base: 18 North American fraud executives)



Source: Aite-Novarica Group survey of 18 North American fraud executives, October 2021

These kinds of programs will likely become more common as scam activity increases and FIs struggle to deploy mitigation strategies that don't depend on complex and costly technological investment. There are a few considerations to weigh for FIs contemplating whether and how to deploy this practice as a mitigation strategy. Most of these considerations center around how to target and customize the program for optimal performance; they are of particular interest to many fraud executives who believe that these kinds of programs, while necessary, are often disappointing in terms of the degree to which they prevent attacks and losses.

There are valid reasons for taking a relatively dim view of the effectiveness of awareness and education programs, of course. Still, it's helpful to make a more informed judgment on the matter by placing it in the proper context of how the programs are structured and deployed. Most fraud executives cite the phenomena of human nature to think that bad things only happen to other people as the root cause for why these programs are less than optimally effective. As an illustration, one fraud executive explained that they'd been challenged to encourage their consumers to engage meaningfully with proactive awareness campaigns because most don't pay attention to efforts that alert them to the potential risks of scams until after they've been victimized. This is a perfectly valid observation and is useful in explaining a certain foundational level of customer apathy. In other words, it's reasonable to assume that there will always be a portion of customers who will remain uninterested in communications from the FI on this matter. The challenge lies in determining how best to position the communication, segment out different target audiences, and deploy the content in such a way that supports optimal engagement.

Position the Program

There are a variety of headwinds to security awareness programs, but perhaps the one fraud executives cite most often is a bias among stakeholders and marketing and communications officers within the FI toward avoiding topics that might make their customers uncomfortable or undermine the relationships they've so carefully cultivated. They are understandably hesitant to discuss something as unpleasant as being scammed and concerned that bringing the topic to the customer's attention might make them think that the FI has little confidence that they can protect the customer from harm. The overwhelming preference is to protect the narrative of communications from uncomfortable topics and avoid triggering the customer into thinking that the FI's performance in protecting them from financial predators is anything short of terrific.

The overall level of scam activity can significantly impact the degree to which one or more segments of the FI's customers are anxious about falling victim to fraudsters. Scam trends in the U.K. provide a useful juxtaposition between approaches in a market nearly saturated with scam activity and approaches in the U.S. where scam activity, while growing, has yet to fully penetrate the public's consciousness.

On examining a variety of scam awareness communications from U.S. FIs, it's hard not to notice the careful and tentative nature of the communications. They avoid sounding alarmist and use verbiage that is technical in nature and clinical in its delivery. It's also hard not to notice that these communications are relatively infrequent and often deeply buried in corporate websites. In contrast, communications from U.K. FIs are much more frequent, are high profile, and often use much more direct verbiage that is less technical and often delivered in a manner that is noticeably more attention-grabbing than in the U.S. This difference is based largely on the notion that the banking public in the U.K. is exposed to a lot more media attention on the matter. For example, HSBC's recent social media campaign features a video of a magician demonstrating to passersby how scammers use social engineering and other techniques to deceive victims into revealing sensitive information or making fraudulent payments (Figure 14).[13]

FIGURE 14: SCREENSHOT FROM HSBC'S RECENT SCAM AWARENESS CAMPAIGN

Source: YouTube

The video is polished, uses straightforward language and thoughtfully scripted segments, and explains the subject matter in an engaging and digestible manner without scaremongering or being alarmist. Consumers in the U.K. could be more receptive to these kinds of communications due to elevated rates of scam activity relative to consumers in the U.S., but it's difficult to imagine that catchy, professional

[13] "Fraud: Don't Miss a Trick, HSBC UK," YouTube, October 14, 2021, accessed March 1, 2022, https://www.youtube.com/watch?v=iud3uNsKnal.

messaging on the same topic wouldn't be more effective than the often clinical and banal campaigns common in the U.S.

Target Effectively

Not all customer segments are equally receptive to communications. Consider the difference between consumers and commercial customers in the U.S. market. While scams have always been a nuisance for consumers, their frequency and severity have only recently increased to the point at which it threatens to become a top-of-mind concern for consumers. Compare this with corporate customers, which suffered from a comparably high rate of BEC attacks for the better part of the last decade. Fraud executives consistently, if anecdotally, report higher engagement rates among corporate customers in proactive security communications than among consumers. Several fraud executives have reported that corporate customers have demonstrably greater rates of engagement with email communications, and enrollment and attendance rates for hosted seminars on the topic. It's not uncommon, therefore, for FIs to start their efforts with corporate customers before expanding the programs into their consumer segments.

Customize Deployment for Optimal Engagement

Few FIs can justify a budget for highly polished, professionally produced videos and ad campaigns that don't directly tie to increased revenue. Some FIs, therefore, focus their efforts on customizing their programs to target discrete customer segments. Others experiment with more creative approaches to promoting awareness of threats or encouraging customers to be more proactive in protecting themselves from attack.

Through its innovation lab, one large FI in the U.S. leveraged a collaborative team consisting of fraud executives, digital- and contact-center channel executives, and product and marketing executives to explore using nudge theory and gamification in their online banking mobile apps to encourage their users to adopt the kinds of security practices that make them a less attractive target for scammers.[14] This effort remains mainly an experiment for now. However, were it deployed into production, it would likely entail custom homegrown technologies, which often come with hefty price tags. That being said, some solution providers are beginning to emerge with innovative ways of incorporating dynamic interactions with customers based on risk-based signals analysis.

[14] See Aite-Novarica Group's report Client Experience Trends in Fraud: Navigating a Busy Intersection, December 2020.

SCAM DETECTION SOLUTIONS

The state of the art of scam detection is still quite primitive, but the landscape of solutions geared for detecting scams is evolving. The rate of consumer payment fraud scams is notably higher in the U.K., so it's not surprising that fraud executives and solution providers that operate there would have insights into existing and emerging trends.

Most of the solutions that are available today span a spectrum of controls. On one end of the spectrum are those meant to conform to requirements under programs like Confirmation of Payee. Adjacent to these are solutions evolving to detect scams via interactive interventions that prompt users to reveal tell-tale indications that they've been deceived. Others seek to incorporate and integrate peripheral layers of signal detection tuned to detect behavioral or transactional anomalies that are predictive of scam activity, particularly when accumulated and combined with several other signal patterns by a centralized risk engine platform. Finally, some solutions seek to exploit the networked nature of the linkage between scams and mule accounts.

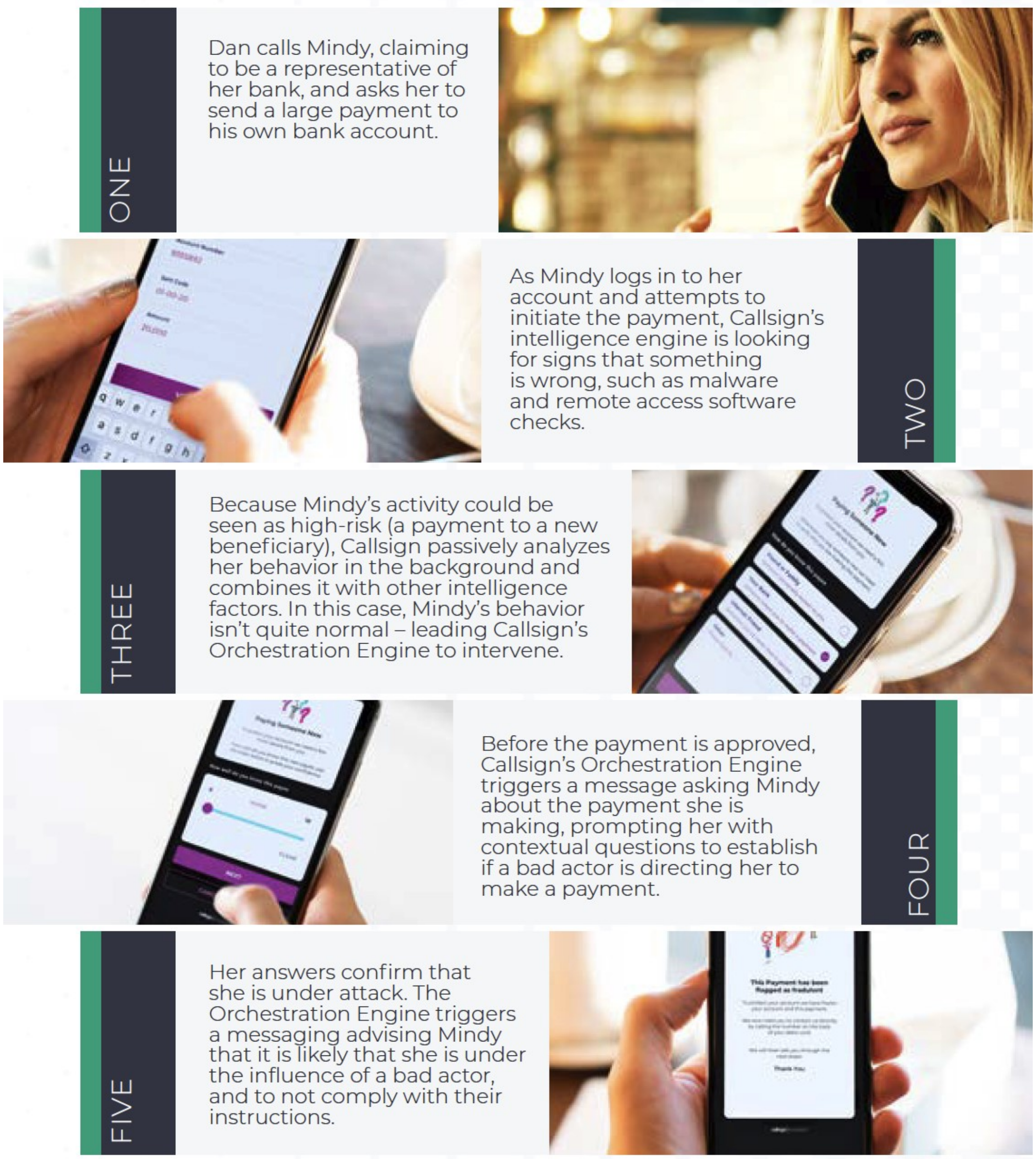
Confirmation of Payee and Interactive Interventions

Many FIs have deployed changes to their online and mobile apps to conform to the requirements under the Confirmation of Payee program. Many fraud executives outside the U.K. have taken an interest in observing this trend despite mixed reports on the effectiveness of the tools in preventing losses by fraud executives in the U.K. Critics of the performance of the program point to a phenomenon known as "alert fatigue" as the root cause for a lackluster performance. Alert fatigue is the tendency for users who are repeatedly bombarded by alerts or warning prompts to become inured to admonishments out of frustration of having the flow of their interaction disrupted or out of irritation stemming from a history of false alarms in previous interactions.

One large FI in the U.K. analyzed the performance of its confirmation of payee controls and found that APP fraud losses increased by 5% and romance scam losses increased by 17%, but invoice scam losses decreased by 28%. The fraud executive who commissioned the analysis concluded that the solution is effective at isolating errors in payments but that it performs poorly as a means of preventing APP scams.

Related to confirmation of payee solutions are those that seek to trigger risk-based interventions to reveal additional risk indicators. Callsign, a global identity fraud detection and orchestration solution provider based in the U.K., has devoted considerable effort to innovating scam detection capabilities that incorporate nudge theory. Its Dynamic Interventions product, launched in early 2021, accumulates a variety of channel and transactional signals for use by multiple risk models to render a risk score that conditionally triggers a prompt in the user's session that introduces a context-specific question. The consumer can respond to this "nudge" by answering the question. The response then triggers the solution to release or block the interaction (Figure 15).

FIGURE 15: CALLSIGN'S DYNAMIC INTERVENTIONS PRODUCT



ONE

Dan calls Mindy, claiming to be a representative of her bank, and asks her to send a large payment to his own bank account.

TWO

As Mindy logs in to her account and attempts to initiate the payment, Callsign's intelligence engine is looking for signs that something is wrong, such as malware and remote access software checks.

THREE

Because Mindy's activity could be seen as high-risk (a payment to a new beneficiary), Callsign passively analyzes her behavior in the background and combines it with other intelligence factors. In this case, Mindy's behavior isn't quite normal – leading Callsign's Orchestration Engine to intervene.

FOUR

Before the payment is approved, Callsign's Orchestration Engine triggers a message asking Mindy about the payment she is making, prompting her with contextual questions to establish if a bad actor is directing her to make a payment.

FIVE

Her answers confirm that she is under attack. The Orchestration Engine triggers a messaging advising Mindy that it is likely that she is under the influence of a bad actor, and to not comply with their instructions.

Source: CallSign

Another provider, Regutize, is developing a solution for automating financial crime investigations, primarily focusing on anti-money laundering (AML). There are two ways that its approach is notable for scam detection:

- Because the primary focus is to reduce false positives, it has emphasized modeling good user patterns through various proprietary techniques.
- If an event does not fit properly into one of its modeled patterns, then the event is flagged as one that requires prompting the user to acquire additional context through a proprietary intervention designed to capture additional information.

The aim is to automate false-positive reduction in alerts produced by the FI's existing control framework. Such an approach has often proven to be useful for automating triage and resolution. This is particularly applicable to scam detection, as high rates of false positives often plague existing control solutions, often because the solution lacks contextual information surrounding the event.

Behavioral Biometrics and Orchestration With Risk Engine Platforms

Some practitioners in the U.K. have reported success with using behavioral biometrics solutions to detect scams. BioCatch, a global behavioral biometric solution provider, has invested research and development efforts into modeling specific patterns of behavior that are predictive of scam scenarios. Some practitioners in the U.K. who have used behavioral biometric solutions to detect scams point out that the predictive performance of these tools is much improved if combined with other indicators accumulated from other channel signals and transactional profile patterns. One fraud executive from the U.K. revealed efforts underway to orchestrate its behavioral biometric signals with transactional profiles using Feedzai as a risk engine capable of scoring the risk of potential scams and triggering intervention treatments in real time.

Scam attacks are highly dynamic by nature, and the signal patterns necessary to detect them are often exceptionally rare and relatively weak in and of themselves. It should come as no surprise, then, that machine learning platforms would be well-positioned to orchestrate the layers of risk models necessary to render such a sophisticated risk decision. As scam activity increases, more FIs will likely turn to an architectural pattern of approach, similar to the one that the U.K. fraud executive outlined, in their efforts to address gaps in their scam control frameworks. This trend may be amplified or accelerated if the trajectory of regulatory scrutiny and market sentiment continues to arc in the direction of expanded consumer protections and demand for improved security protections.[15] This will likely be a driver in the growing market for machine learning solution providers. Table F lists machine learning platform vendors.

TABLE F: MACHINE LEARNING PLATFORM VENDORS

FIRMS		
ACI Worldwide	Acuant, a GBG company	Symphony AyasdiAI
BAE Systems	Bleckwen	Bottomline Technologies
Brighterion	DataVisor	Featurespace
Feedzai	FICO	GB Group (GBG)
Genpact	IBM	Inform GmbH
iSOFT	LexisNexis Risk Solutions	NetGuardians
NICE Actimize	Oracle	Pelican
PwC	Quantexa	Risk Ident
SAS	Similty	ThetaRay
TigerGraph	Tookitaki	Verafin

Source: Aite-Novarica Group

Scam Detection by Way of Link Analysis

Another notable pattern that solution providers and practitioners have found useful in detecting scam attacks is linking one or more identifying characteristics associated with a suspected scam attack to identifying characteristics of reported mules or fraudsters. The LexisNexis ThreatMetrix platform from LexisNexis Risk Solutions is a widely

[15] See Aite-Novarica Group's report Fraud & AML Machine Learning Platforms: Financial Crime Detection's Next Frontier, August 2021.

adopted, consortia-based identity authentication and verification solution. The solution leverages its sizeable network of device characteristics linked with personas tagged with markers that indicate whether the persona has been associated with fraud by others in the consortium. Practitioners—mainly in the U.K.—have had success leveraging the solution to detect potential scams by scoring the risk of outbound payments according to linkages between the payee's account or device characteristics and the account or device characteristics of personas reported as mules or fraudsters by others in the consortium.

Other solutions work in a similar manner but differ slightly in their approaches and where they fit in the chain of events surrounding a scam. Mastercard's Vocalink platform, for example, is a network-oriented solution that is particularly well-suited to reveal risk indicators that emerge in the pattern that a fraudulent payment makes after it leaves the victim's account. Vocalink may not detect the scam in time to trigger a preventive intervention, but it nonetheless serves a useful function. The solution's utility is in revealing the mule activity that follows the initial scam and in arresting the chain of events in such a way that disrupts the criminal logistics network. This is a valuable service and is vital to the sorely needed reforms to be made in how FIs manage recoveries and collaboration in the era of faster payments.

COLLABORATION EFFORTS

In her opening remarks of U.K. Finance's 2021 mid-year fraud report, Katy Worobec summarized the challenge that scams pose to consumer and commercial bank customers well by stating, "The banking sector cannot solve this on its own—there must be a coordinated approach adopted across every sector if this is to be tackled effectively."[16]

Technological and policy-based mitigation strategies can only go so far in effectively preventing scams from making a profoundly negative impact on the client experience and losses resulting from scam activity. So long as fraudsters continue unchallenged in their efforts to organize and collaborate on their criminal operations on social media platforms and exploit security vulnerabilities in mobile phone networks and email platforms, and so long as law enforcement remains overwhelmed with caseloads for which they're prevented from imposing penalties on the growing ranks of smaller rings

[16] "2021 Half Year Fraud Update," U.K. Finance, September 2021, accessed January 31, 2022, https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2021-FINAL.pdf.

and independent actors, then scams will continue to grow. It's Important, therefore, that leaders in the financial services industry start taking steps now to draw more attention to this challenge. They must forge ahead with collaborative efforts within the industry, the market, and with regulators as well as networks, telecommunications companies, social media companies, and law enforcement. A variety of nonprofit organizations exist to foster this kind of collaboration, including The Knoble, the National Cyber-Forensics and Training Alliance (NCFTA), the Bank Policy Institute's BITS Fraud Working Group and Steering Committee, and the Financial Services Information Sharing and Analysis Center (FS-ISAC), to name a few.

There are precedents that are instructive in terms of what benefits could be achieved. In response to the rising tide of BEC attacks several years ago, the FBI created a program informally known as the "kill chain" process. This effort was borne out of feedback from FIs to improve the bureau's effectiveness at recovering stolen funds from BEC attacks that find their way overseas, as most do. The bureau focused primarily on growing the breadth and depth of contacts in local jurisdictions in Hong Kong and Dubai. It wasn't long before FIs saw improvements in recovery rates from those locations. Granted, the kill chain process works best if the victim notifies the bureau of the fraud within 24 hours of occurrence. Still, when those conditions are met, recovery rates were markedly improved over the period before the program.

Another interesting development to watch is a legislative effort in the U.K. that seeks to impose financial penalties on social media companies that fail to detect and prevent criminal rings operating on their networks linked to scam losses by consumers.

CONCLUSION

Scams have grown from relatively minor irritations to a considerable challenge. Much must be done and much needs to happen before the problem can be considered to be properly known and managed. There is much to learn from the experiences in the U.K.:

- Scams are more properly tracked and categorized in the U.K. than in the U.S. and other markets. Collaborating on a more consistent means of categorization and measurement would benefit the industry's ability to make a compelling case for a holistic and collaborative approach to addressing the risk.

- Scam attacks have grown consistently over many years in the U.K., where losses are now larger in scale than card fraud losses. Growth in scam activity in consumer and commercial customer portfolios is spreading to other markets and is raising concerns about whether the same patterns that emerged in the U.K. will impact regulatory pressure on reimbursement policies and public sentiment.

- Efforts spanning technological detection and prevention strategies to voluntary and regulatory programs aimed at making reimbursement policies more consistent and more consumer-friendly in the U.K. are being scrutinized to determine what lessons can be learned from practitioners in markets where scams have only recently begun to garner significant attention.

- Recent bulletins from the CFPB have caught the attention of many fraud executives in the U.S., particularly those whose FIs rely on conditional circumstances in their terms of use contracts that have, until recently, shielded them from assuming liability for ATO losses, many of which are the result of harvesting scams.

- The fallout from the CFPB's bulletins has yet to take shape, but many fraud executives will be working with their compliance and legal counsel to prepare to change or defend their policies. For many, this has the potential to increase total fraud losses and compliance costs.

- There are a variety of mitigation strategies for scams, but the consensus among fraud executives is that most perform poorly if they are not orchestrated with others in a layered framework.

RELATED AITE-NOVARICA GROUP RESEARCH

Top 10 Trends in Fraud & AML, 2022: Braving the New Normal, January 2022

Aite Matrix: Leading Fraud & AML Machine Learning Platforms, December 2021

Trends in Fraud in the Digital Channel: Fraud Inc. Pivoting to Scams, December 2021

Aite-Novarica Group's Fourth Annual Financial Crime Forum: Outpacing Fraud and Financial Crime, November 2021

ABOUT AITE-NOVARICA GROUP

Aite-Novarica Group is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

CONTACT

Research and consulting services:
Aite-Novarica Group Sales
+1.617.338.6050
sales@aite-novarica.com

Press and conference inquiries:
Aite-Novarica Group PR
+1.617.398.5048
pr@aite-novarica.com

For all other inquiries, contact:
info@aite-novarica.com

Global headquarters:
280 Summer Street, 6th Floor
Boston, MA 02210
www.aite-novarica.com

AUTHOR INFORMATION

Trace Fooshée
+1.857.406.3515
tfooshee@aite-novarica.com

Research Design & Data:
Judy Fishman
jfishman@aite-novarica.com