FS-ISAC

Threat Information Sharing and GDPR: A Lawful Activity that protects Personal Data

By: White and Williams LLP and Osborne Clarke LLP

White and Williams LLP

Osborne Clarke

FS-ISAC

Threat Information Sharing and GDPR

Table of Contents

FS-ISAC

Threat Information Sharing and GDPR

Executive Summary

In the world of data security and data privacy, cyberattacks continue to increase in number and sophistication, presenting significant challenges for organizations required to ensure the security of their data and systems. Threat information sharing protects organizations by allowing them to better detect threats and mitigate vulnerabilities in their networks and systems against cyberattacks. This paper concludes that threat information sharing by FS-ISAC and its member organizations ("Members") is a lawful practice under Article 6(1)(f) of the European Union General Data Protection Regulation, Regulation (EU) 2016/679 ("GDPR"). Article 6(1)(f) of GDPR states that processing personal data is lawful when it "is necessary for the purpose of the legitimate interests pursued by the controller or by a third party." The processing of personal data under this Article must meet a three-step test: legitimacy, necessity, and a balancing of interests. This paper outlines how the processing of personal data in threat information by FS-ISAC and Members meets this criteria.

- FS-ISAC's and its Members' interests – trying to prevent fraud and improve network security against cyberattacks – are legitimate under GDPR.
- The processing of personal data for these interests is necessary and proportionate as a critical component of ensuring network and system security and the prevention of fraud.
- The interests are balanced because various factors, including privacy safeguards adopted by FS-ISAC and its Members, work to ensure that the interests of preventing or stopping fraud and ensuring the security of financial institutions' networks are not outweighed by the interests of the data subjects whose personal data is processed. Indeed the interests of data subjects are aligned with those of FS-ISAC and Members in many cases.

Section I of this paper introduces threat information sharing under GDPR, while Section II discusses ISACs, the types of personal data and non-personal data comprised in threat information, and traffic light protocol. Section III discusses threat information sharing under GDPR's framework, including the role of FS-ISAC and its Members as data controllers and/or data processors. Section IV concludes that threat information sharing satisfies Article 6(1)(f) because the interests served by threat information sharing are legitimate, the processing of personal data is necessary and proportionate, and the interests are not outweighed by the interests and rights of data subjects. Section V concludes that threat information sharing is lawful under GDPR.

I. Introduction

In the world of data security and data privacy, cyberattacks continue to increase in number and sophistication, presenting significant challenges for organizations required to ensure the security of their data and systems. Threat actors include autonomous attackers, groups operating as part of a criminal enterprise, nation-states, and even individuals. As a means to combat and mitigate these threats, government agencies, businesses, and ISACs share with each other information concerning cyber threats to improve their security posture. Vulnerabilities and incidents are rarely specific to one organization only. By employing effective threat information sharing, particularly between organizations of a similar nature, an active threat actor will have only one opportunity to attack a system with success,as threat information shared in real-time will pre-warn other organizations and enable them to mitigate vulnerabilities in their networks and systems to foil a subsequent similar attempt by the same or copycat actor. Sharing threat information is a critical tool employed by organizations and critical industries in defending against cyber threats and protecting data, including personal data of data subjects.
On May 25, 2018, GDPR took effect across the EU, implementing the most significant regulatory change in data protection in more than 20 years. The foundational principle of GDPR is that the protection of "personal data" is a fundamental right of natural persons. GDPR has a far-reaching effect in terms of both the vast amounts of information it regulates and the legislation's extra-jurisdictional, global reach. As a result, GDPR has a clear impact upon the landscape of international threat information sharing. Yet, both GDPR and international threat information sharing have the same goals. In fact, the goals and purposes of threat information sharing – to preserve networks, systems, and associated personal data from unauthorized acquisition, alteration, or loss – are a cornerstone of GDPR and serve to protect the fundamental rights and freedoms of individuals in respect of their personal data.This paper explains how threat information sharing is a legitimate and lawful process under GDPR. Article 6(1)(f) states that the processing of personal data is lawful when it "is necessary for the purpose of the legitimate interests pursued by the controller or by a third party." Threat information sharing by an ISAC, including FS-ISAC and its Members squarely falls within this criteria. Threat information sharing is critical for ensuring network and system protection, the prevention of financial fraud, and for identifying criminal activity. Threat information sharing, and the processing of personal data within threat information, is performed for the legitimate interests of ISACs, their members, as well as the interests of third parties including governments, consumers, and data subjects whose personal data may be targeted by threat actors. Such processing also is necessary to achieve such interests, and is proportionate. It also satisfies Article 6(1)(f)'s balancing test, which weighs the legitimate interests against the rights and interests of the data subjects whose personal data is processed. It drives at fundamental goals of GDPR to protect personal data and prevent collateral human harm sustained at the hands of threat actors.

II. Threat Information Sharing and Types of Information Shared

A. ISACs and Threat Information Sharing

Cyberattacks and cyberterrorism endanger the welfare of EU organizations, its economy, and its citizens. "In the context of widespread cybercrime, users cannot fully enjoy protection of data without effective cybersecurity. Therefore, the need for security and the exercise of the fundamental right to data protection are complementary."1 The European Commission, in its 2016 Communication to the European Parliament, The Council, The European Economic and Social Committee, and the Committee of the Regions, stated that "[e]very day, cybersecurity incidents cause major economic damage to European businesses and the economy at large," resulting in "economic losses of hundreds of billions of euros each year."2 It is increasingly important that organizations share threat information to improve their security posture. Two realities drive this self-evident conclusion: (1) the growing sophistication of techniques used by threat actors to perpetrate fraud, steal information, disrupt services, or undertake other cyberattacks; and (2) the expanding interconnectivity of global networks, infrastructure, and financial systems. As noted last year by ENISA's Executive Director, "Everything is connected. And everything needs to be secure."3 Threat information sharing addresses these concerns by enabling organizations to collectively identify cyber threats and take preventive action against imminent cyberattacks by mitigating and patching vulnerabilities.

Threat Information Sharing is the exchange of information relating to threats, whether cyber or other, between members of a sharing community for the purpose of enhancing their security posture by leveraging the collective knowledge, experience, and capabilities of the community toward the threat.
4 Generally, a "threat" is any circumstance with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), assets, individuals, other organizations, or a nation through an information system "via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service."5 Threat information is information related to a threat that might help an organization protect itself or others against a threat or a threat actor. Threat information sharing involves the sharing of information to help organizations protect individuals, organizations, nations, and even the public at large against malicious acts resulting in an unauthorized access, disclosure, loss, or alteration of data, including personal data.

A common motto for threat information sharing is allowing "one organization's detection to become another's prevention."6 Vulnerabilities and incidents are rarely specific to one organization.7 A security breach into one organization's network or system can provide hackers with the ability to breach the security of another organization by using the same tactics, techniques, and procedures ("TTPs"), thereby potentially initiating a chain of security breaches compromising multiple networks and systems of numerous organizations. A chain of security breaches, in turn, potentially compromises vast amounts of personal data held by those organizations.8 Thus, a key goal of threat information sharing, particularly between organizations of a similar nature or industry, is that the threat actor will have only one

2 The European Commission, Joint Communication To The European Parliament, The Council, The European Economic and Social Committee, and The Committee of The Regions, Strengthening Europe's Cyber Resilience System and Fostering Competitive and Innovative Cybersecurity Industry [2016] ("EC Communication on Strengthening Europe's Cyber Resilience"), at 2, available at
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0410&from=EN.

3 Helmrecht, EU Strategies to Secure the EU Cyber Space and Critical Infrastructure Against Hackers [2017], at 3, available at
https://www.enisa.europa.eu/publications/ed-speeches/eu-strategies-to-secure-the-eu-cyber-space-and-criticalinfrastructure-against-hackers.

4 E.g., Johnson et al., Guide to Cyber Threat Information Sharing, [2016], NIST Special Publication 800-150, available at:
http://dx.doi.org/10.6028/NIST.SP.800-150.

5 Id.

6 Id.

7 Andrew Cormack, Incident Response: Protecting Individual Rights Under GDPR, Scripted, Vo. 13, Issue 3 [Dec. 2016] at 263, available at
https://script-ed.org/wp-content/uploads/2016/12/13-3-cormack.pdf.

8 Nick Ismail, The Enemy of My Enemy Is My Friend: Sharing Intelligence to Combat Data Theft, [2017] Information Age, online source, available at:
http://www.information-age.com/sharing-cyber-threat-intelligence-necessary-combat-data-theft-123467953/.

opportunity to attack a system because threat information sharing will prevent the same or a copycat threat actor from breaching a second organization using the same means.9 Knowing how a cyberattack was conducted and discovered can help other organizations detect or prevent the same attacks happening to them.10 ISACs are a critical tool to advance this goal, and serve an important function to protect and maintain the security and privacy of networks, systems, and associated personal data therein.

ISACs are "non-profit organizations that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure)" to allow the sharing of threat information between the private and the public sector.11 Sometimes oriented on a specific, critical sector (e.g., financial services, health, energy) or focal point (e.g., national level), ISACs attract members to establish communities within the private sector to gather and analyze information about cyber threats and incidents. FS-ISAC is a worldwide ISAC, including in the EU, for the financial services sector, a sector highly exposed to cyber-threats and cyber-crime because "[a] successful attack on the financial infrastructure gives the criminals access to money and results in loss of trust, not only for a single bank but for the whole sector and services it delivers (e.g., electronic payments)."12

1. The Traffic Light Protocol Used by ISACs to Restrict Dissemination of Information When sharing threat information, ISACs and their members, including FS-ISAC and its Members, employ the Traffic Light Protocol ("TLP"). TLP is a set of designations used to ensure that dissemination of confidential or sensitive information is restricted to appropriate audiences based on the sensitivity of the information and its source.13 TLP provides a simple and intuitive structure for indicating the sensitivity of information and when/how the information may be shared. Its purpose is to ensure necessary and proportionate use of threat information, including any personal data contained therein.

TLP employs four colors to indicate sharing and dissemination restrictions: Red, Amber, Green, and White. Generally, the designations and their restrictions are as follows:

- TLP:RED – Recipients may not share TLP:RED information with parties outside of the specific exchange in which the information originally was disclosed.

9 Neal Ziring in Tom Spring's NSA Advocates Data Sharing Framework, [2017], Threat Post, available at: **https://threatpost.com/nsa-advocates-data-sharing-framework/126495/.**

10 Cormack, Incident Response: Protecting Individual Rights Under GDPR, at 263.

11 See European Network and Information Security Agency ("ENISA"), Cooperative Models for Information Sharing and Analysis Centers (ISACS) [2018] (hereinafter, "ENISA ISAC Paper"), at 7. ISACs originally were created by Executive Order of President Clinton following the first terrorist attack on the World Trade Center (1993) and the Oklahoma City terrorist attack (1995). Today, in the United States, twenty-three sector-based ISACs comprise the National Council of ISACs ("NCI"), which collects, analyses, and shares cyber and physical threat intelligence with member companies in their particular sectors. The following discussion of ISACs is based in part on the ENISA ISAC Paper.

12 ENISA ISAC Paper at 27.

13 US-CERT, Traffic Light Protocol (TLP) Definitions and Usage, available at **https://www.us-cert.gov/tlp.**

- TLP:AMBER – Recipients may share TLP:AMBER information only with members of their own organization, or with their clients or customers who need to know the information to protect themselves or prevent further harm.
- TLP:GREEN – Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not by publicly accessible channels. Information in this category may be circulated widely within a particular community, but may not be released outside of the community.
- TLP:WHITE – Recipients may share TLP:WHITE information without restriction.14

The color designation is set by the initial sharing ISAC member that serves as the source of the information. Threat information, including any personal data therein, is protected from dissemination and disclosure pursuant to the restrictions of the TLP designation.

2. Categories of Information Shared by ISACs

A majority of information processed by ISACs during the sharing of threat information is not personal data. Article 4(1) of GDPR defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." Personal data may includemany information that relates to an identified or identifiable living individual, even if unconnected piecesm of information, when collected together, can lead to the identification of a particular person.15 However, when sharing threat information, ISACs primarily exchange information about threats; incidents (detailsabout successful attacks and categories of information affected); vulnerabilities describing weaknesses in systems, processes, software, or hardware; mitigating measures to correct vulnerabilities or defend against threats and incidents, such as installation of software patches; and best practices regarding items like security controls, incident response practices, and software patching.16 They also exchange Indicators, TTPs, Security Alerts, Threat Intelligence Reports, and Tool Configurations – all categories of information that often do not contain personal data. These informational items are defined as follows:

- Indicators – technical artifacts or observables, including Domain Name System (DNS) domain name, a Uniform Resource Locator (URL), or the subject line text of a malicious email, that suggest an imminent or ongoing attack;

14 US-CERT, Traffic Light Protocol (TLP) Definitions and Usage.

15 GDPR, Article 4(1); European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-doesgeneral- data-protection-regulation-gdpr-govern_en. If data has been partially anonymized or "pseudonymised," but can be combined with other information to re-identify a person, the data remains "personal data" for the purposes of GDPR. However, if personal data has been truly and irreversibly anonymized (i.e. rendered anonymous in such a way that the individual can no longer be identified, including in combination with other data), then such data is no longer considered personal data for the purposes of GDPR.

16 ENISA ISAC Paper at 31.

- **Tactics, Techniques, and Procedures ("TTPs")** – details of the behavior of threat actors, such as tendencies, attack tools, and delivery mechanisms;
- **Security Alerts** – also known as advisories or bulletins, that provide brief technical notices on systems' current vulnerabilities, exploits, and other security concerns;
- **Threat Intelligence Reports** – prose reports describing TTPs, types of systems exploited, and types of information targeted, as well as other threat-related information that provides greater situational awareness to an organization; and
- **Tool Configurations** – recommendations for setting up and using mechanisms that support automated collection, exchange, processing, analysis, and use of threat information, such as how to customize intrusion detection signatures or firewall rules.17

These categories of information typically do not contain personal data.

3. Types of Personal Data that May Be in Threat Information For the purposes of this paper, FS-ISAC assumes that the processing and sharing of threat information by FS-ISAC and its Members sometimes involves "personal data," as defined under Article

4(1). To the extent that data processed in threat information sharing includes personal data, such personal data most often consists of email addresses and IP addresses. Less often, the data could include names and bank account/credit card information of victims, or the names of threat actors themselves.18 Importantly, all information shared, including any personal data, is subject to the TLP restrictions. Personal data processed and shared for the purpose of threat information sharing may be broken down into three categories: Falsified Personal Data – when an identity, or a partial identity, has been created and used by someone who is hiding their identity behind the falsified personal data ("Falsified Personal Data").
Stolen/Victim Personal Data – when a third party has stolen the personal data of an actual data subject ("Stolen Personal Data").

17 Johnson, Guide to Cyber Threat Information Sharing.

18 Whilst there is some debate in the threat information sharing community (and beyond) as to whether IP addresses will always consist of personal data, because IP addresses and online identifiers can be considered personal data under GDPR if an individual can be identified from such information, for purposes of this paper, FS-ISAC treats IP addresses as personal data. See, e.g., C. Sullivan & E. Burger, "In The Public Interest": The Privacy Implications of International Business-to-Business Sharing of Cyber-Threat Intelligence, Computer Law & Security Review, Vol. 33, Issue 1 at 14-29 (2017). FSISAC has not considered the processing of special categories of personal data under Article 9(1) in the context of threat information sharing because it is highly unlikely that any personal data processed by FS-ISAC and its Members would constitute a special category of personal data.

Personal Data of Threat Actors – the personal data of the individuals committing fraud or other crimes ("Threat Actor Information").

Falsified Personal Data. Threat information sharing involves Falsified Personal Data when an identity, or a partial identity, has been created and used by the threat actor or other member of the criminal conspiracy to hide their real identity behind false data (i.e., data about a non-existent data subject). This Falsified Personal Data is collected by a Member, Regulatory Authorities, or by Law Enforcement, and then transmitted to FS-ISAC using the TLP restrictive measures. Adhering to that protocol, FS-ISAC in turn transmits the data to other Members, Regulatory Authorities, and Law Enforcement to accomplish the purpose of identifying the threat actors for the purpose of preventing fraud, increasing organizations' networks and systems security against a growing threat, and/or to identify potential criminal activity or threat to the public at large. Thus, Falsified Personal Data may constitute personal data under Article 4(1) because it may be used to identify the threat actor hiding behind the false details.

Stolen/Victim Personal Data. Identity theft and financial fraud are worldwide problems and growing.19 Threat information sharing may involve Stolen/Victim Personal Data when a third party has stolen the personal data of an actual data subject (i.e., the victim). When a Member, Regulatory Authority, or Law Enforcement detects the fraud, it collects the fraudulently-used personal data, and transmits it to FS-ISAC using the TLP measures with the intent to prevent further fraud or identify criminal activity. Complying with that protocol, FS-ISAC in turn transmits this personal data to other Members, Regulatory Authorities, and Law Enforcement to accomplish the purpose of assisting other member financial institutions, Regulatory Authorities, and/or Law Enforcement to prevent further fraud and harm suffered by the actual data subject whose personal data is being misused.

Threat Actors Personal Data. Threat information sharing involves Threat Actor Personal Data when the identity, or partial identity, of an individual committing fraud or other crimes is discovered. A Member, Regulatory Authorities, or Law Enforcement detects the person committing the crimes, collects personal data about the threat actor committing the crimes, and with the intent to prevent further crimes from being committed, transmits the Threat Actor Personal Data to FS-ISAC using the TLP. Complying with that protocol, FS-ISAC in turn transmits the Threat Actor Personal Data (i.e., the personal data of the person committing crimes) to other Members, Regulatory Authorities, and/or Law Enforcement for the purposes of preventing further crimes and potentially allowing Law Enforcement to bring the threat actor to justice under EU law or the law of other jurisdictions.

4. Satisfying transparency requirements

Because of the nature of the personal data and the purposes of threat information sharing, GDPR's transparency requirement for processing these three categories of personal data under Articles 12-14 is met. Articles 13 and 14 enumerate specific notification obligations with which data controllers must comply when processing a data subject's personal data. These provisions include a

19 E.g., European Commission, Joint Communication To The European Parliament, The Council, The European Economic and Social Committee, and The Committee of The Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013], at 9 ("Cybercrime is one of the fastest growing forms of crime, with more than one million people worldwide becoming victims each day."), available at http://eeas.europa.eu/archives/docs/policies/eu-cybersecurity/cybsec_comm_en.pdf.

data subject's so-called "right to be informed," and the right to obtain minimum "fair processing information" before a data controller may process the personal data.

Article 13 applies where the data controller obtains personal data from the data subject directly.20 This direct collection is predominantly undertaken by Members, who satisfy the relevant Article 13 obligations by ensuring that their privacy notices provide data subjects with adequate transparency information about how their personal data will be used for threat information sharing. This requirement is not unique to threat information sharing in particular, and so it does not expose Members to any new compliance burden. 21 To the extent FS-ISAC obtains personal data directly from the data subject – a very rare occurrence – this is covered in FS-ISAC's own privacy notice.

Article 14 applies where FS-ISAC and Members receive data indirectly or from alternative sources.22 The application of this is somewhat different. In particular, Article 14(5) exempts altogether disclosures where they would be impossible or involve a disproportionate effort, or otherwise would likely "seriously impair" the purpose of the processing. Article 14(5)(a) states that disclosures under Article 14 are not required where:

the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.23

In the context of threat information sharing, providing the requisite notice to data subjects of Falsified Personal Data, Stolen/Victim Personal Data, and/or Threat Actor Information could "prove impossible or would involve a disproportionate effort" to trigger the Article 14(5) exemption. Many times, the FS-ISAC and its Members do not know who the data subjects are or have the means and necessary information to contact them. In addition, the notification requirements for the processing of these three categories of personal data would "likely render impossible or seriously impair" the interests and purposes of the threat information sharing altogether, and would "substantially undermine the value and purpose of sharing threat intelligence."24 Indeed, if Article 14(5) did not apply, conceivably FS-ISAC and its Members would need to notify each threat actor that their data has been collected, and explain how it is processed – an action that would undermine legitimate interests of fraud prevention, network and system security, and identifying criminal activities or threats to the public that FS-ISAC and its Members seek to achieve – interests shared with governmental entities, data subjects, and other

20 GDPR, Article 13(1)
.

21 Threat information sharing forms part of a broader security and fraud prevention strategy which Members will already be required to explain to data subjects in their privacy policies as part of wider transparency requirements.

22 GDPR, Article 14(1).

23 GDPR, Article 14(5) (emphasis added).

24 C. Sullivan & E. Burger, "In the public interest": The privacy implications of international business-to-business sharing of cyber-threat intelligence, [2017] Computer Law & Security Review, Vol. 33, Issue 1. pp. [·].

organizations. The effect of such an application of GDPR would undermine the very interests and protections of personal data and data subjects that GDPR seeks to preserve.

Guidance from the Article 29 Working Party25 on GDPR's transparency requirements is illustrative. The guidance states that where banks share individual account holder information with law enforcement authorities for the purposes of complying with anti-money laundering regulations, the Article 14 disclosure requirements, which that otherwise would require the bank to disclose its processing of the shared information to the individual, would seriously impair the purposes of the legislation (which provides the legal basis for the relevant processing activity).26 In such circumstances, the bank may rely on the Article 14(5)(b) exemption for disclosing such processing information. Threat information sharing is analogous. FS-ISAC and Members share threat information that may contain personal data of the threat actors or stolen data. To provide disclosures of such personal data would seriously impair the purposes of the sharing: preventing fraudulent activities and to ensure the security of networks and systems, and/or to identify potential criminal activity: all interests deemed legitimate by GDPR.

Finally, Article 14(5)(b) states that where the exemption applies, "the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available." Similar to the balancing test under the Article 6(1)(f) lawful basis for processing personal data, actions taken by FS-ISAC and its Members, as data controllers, would constitute "appropriate measures" to protect the data subject's rights and legitimate interests, because the processing would be undertaken to prevent fraud, to ensure network security and the protection of data subjects' personal data, and to identify crime. In the case of processing Stolen/Victim Personal Data, the processing of such data could stop an ongoing crime being committed against the data subject and provide a path to restitution.

B. EU Policy Toward ISACs and Threat Information Sharing

Threat Information Sharing and GDPR

The realized importance of threat information sharing and ISACs is becoming more common in the EU. Sectoral ISACs operate in member states (e.g., Poland – the Banking Cybersecurity Centre; Norway – the HealthCERT), and EU-wide (FI-ISAC), as do government-facilitated ISACs in Finland (by the National Cyber Security Centre), Belgium (by the Centre for Cybersecurity Belgium), and other member states.27

- In its 2016 Communication regarding Europe's cyber resilience, the European Commission stated that at the EU level, "Sectoral Information Sharing and Analysis

25 We note that the Article 29 Working Party has now been superseded by the European Data Protection Board.

26 Article 29 Working Party, Article 29 Working Party Guidelines on Transparency Under Regulation 2016/679, pp. 31-32.

27 E.g., ENISA ISAC Paper at 21-23.

28 ENISA ISAC Paper at 7.

Centres (ISACs) and corresponding CSIRTs can play a key role in preparing for and responding to cyber incidents. To ensure effective information flows on evolving threats and to facilitate the response to cyber incidents, ISACs should be encouraged to engage with the CSIRTs Network under the NIS Directive, and with the European Cybercrime Centre at Europol, CERT-EU, as well as with relevant law enforcement bodies."29

- In the same report, the Commission identified three goals: "stepping up cooperation to enhance preparedness and deal with cyber incidents; addressing challenges facing Europe's cybersecurity Single Market; nurturing industrial capabilities in the field of cybersecurity." To achieve these goals, the Commission "decided to facilitate the creation of an 'information hub' to support the exchange of information between EU bodies and Member States."30

- In July 2016, the EU adopted NIS Directive (EU) 2016/1148, which "imposes on the Member States the obligation to establish Computer Security Incident Response Team ('CSIRT') and a competent national NIS authority." The entities covered by this Directive, operators of essential services and digital service providers, are required to notify ofincidents and to take "appropriate and proportionate technical and organizational measures to manage risks posed to the security of network and information systems which they use in their operations." The Directive stressed that "cooperation between the public and private sector is essential."31 In connection with this Directive, ENISA noted that sectoral ISACs can support the smooth implementation of the NIS Directive by being the placeholders for the interaction between the public and the private sector stakeholders.32

- In 2015, the Commission adopted the Digital Single Market (DSM) Strategy, concluding that the DSM strategy denotes "the strategy of the European Commission to ensure access to online activities for individuals and businesses under conditions of fair competition, consumer and data protection."33

- In 2013, in a Communication regarding the cybersecurity strategy for the EU, the Commission noted that "[f]undamental rights, democracy and the rule of law need to be protected in cyberspace," and toward that end, "[t]o promote cyber resilience in the EU,

29 EC Communication on Strengthening Europe's Cyber Resilience at 7, available at **https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52016DC0410&from=EN.**

30 Id. at 3-5.

31 Cormack, Incident Response: Protecting Individual Rights Under GDPR, at 270.

32 ENISA ISAC Paper at 21-23.

33 European Commission, Shaping the Digital Market, Online Source, available at: **https://ec.europa.eu/digital-singlemarket/en/policies/shaping-digital-single-market;** see also ENISA ISAC Paper at 9-10. both public authorities and the private sector must develop capabilities and cooperate effectively."34

III. Threat Information Sharing Under GDPR's Framework

A. GDPR's Far-Reaching Effect

GDPR governs the processing of "personal data" with the aim to protect "fundamental rights and freedoms of natural persons and in particular their right to protection of personal data."35 The law constitutes the most significant change in the data protection regime in the EU in the last twenty years, and its extra-jurisdictional reach is set to have a profound impact upon the operations of organizations around the world. "Processing" is defined in very broad terms to mean "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means."36 This expressly includes any collection, recording, organization, storage, alteration, use, disclosure by transmission, or destruction of data. Thus, the regulation effectively governs any activity carried out with the personal data, subject to its jurisdictional reach as set out in Artic e 3.37 GDPR also defines the sole lawful purposes for processing of personal data.38 If a processing of personal data does not fit within the authorization of GDPR, a data controller and data processor run afoul with the law.

The exact impact of GDPR on international threat information sharing appears not fully understood. There should be no misunderstanding: threat information sharing, undertaken in a proper and controlled manner, is a lawful enterprise under GDPR. Article 6(1)(f) holds as lawful the processing of personal data that "is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject" requiring protection of the personal data. The processing of personal data in threat information by FS-ISAC and its Members, as well as other ISACs, member organizations, and governmental entities meets this criteria.

As discussed further below, the interests of the ISACs, their members, and even the public at large, are legitimate: the interests are lawful, clearly articulated to allow a balancing test against the interests and rights of the data subject, and they represent real, non-speculative interests. The purposes of the processing – to mitigate or prevent a cyberattack – also are legitimate: to prevent fraud, to improve network and information security, and to identify potential criminal activity or threats to public security. Indeed, the purpose of threat information sharing – to preserve networks, systems (and the

34 The European Commission, Joint Communication To The European Parliament, The Council, The European Economic and Social Committee, and The Committee of The Regions, Cybersecurity Strategy of the EU: An Open, Safe and Secure Cyberspace [2013] ("EC Communication on Cybersecurity Strategy of the EU") at 2, 5, available at

http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.

35 GDPR, Art. 4(1) and Art. 1(2).

36 GDPR, Art. 4(2).

37 Generally, GDPR applies only to the processing of personal data (1) in the context of the activities of an establishment of a controller or a processor in the EU; (2) the processing of personal data of an EU data subject that relates to offering the data subject goods or services, or monitoring their behavior in the EU; or (3) where an EU Member State's law otherwise applies by virtue of public international law. See GDPR, Article 3

38 GDPR, Article 6.

personal data contained therein) from unauthorized acquisition, alteration, or loss – is a cornerstone of GDPR's aim to protect fundamental human rights because it serves to protect personal data and prevent any collateral human harm from a personal data breach.

B. FS-ISAC and Its Members as Independent Controllers and Processors

GDPR distinguishes between the actions of data controllers and data processors. Data controllers are those parties, whether acting alone or with others, that determine the means and purposes of data processing. Data processors are those parties that process personal data on behalf of a data controller.39 In the context of threat information sharing, both FS-ISAC and its Members may act as independent data controllers. At times, FS-ISAC also may act as a data processor. The distinction is important under GDPR. The data controller primarily is responsible for ensuring that personal data is processed lawfully in accordance with the regulation, and is required to have a lawful basis to process personal data.

1. FS-ISAC: Sometimes a Controller, Sometimes a Processor

When processing and transmitting personal data within threat information, FS-ISAC sometimes acts as an independent data controller. Sometimes, FS-SAC may serve as a data processor. FS-ISAC acts as a data controller when it:

- carries out trend analysis on threat data shared by its Members;
- retains data (usually with the source of the data removed) for its own purposes; and
- chooses to share it with other ISACs (in compliance with the traffic light protocol set out in FS-ISAC's Operating Rules).

FS-ISAC is a data controller under these circumstances because FS-ISAC determines the processing of personal data without recourse to its Members, notwithstanding the fact that FS-ISAC often shares the outcome of the threat information sharing, and processing of "personal data" therein, with its Members in due course.

FS-ISAC may also serve as a data processor when FS-ISAC processes personal data contained in threat information solely for purposes of facilitating threat information sharing between its Members (i.e., via its portal and other threat information sharing tools). FS-ISAC acts as a data processor on behalf of the Member who initially shared and supplied the information. FS-ISAC processes the personal data pursuant to documented and required procedures between the parties contained in FSISAC's Operating Rules (which include the requirements of Article 28). In such circumstances, FSISAC does not render any significant independent decisions regarding the means or purpose of processing the data. FS-ISAC also undertakes the processing of certain data on behalf of Members (1) subject to the Members' instructions; (2) while maintaining appropriate technical and organizational measures to protect the data; and (3) agreeing to assist Members with any supervisory authority or data subject requests.

39 GDPR, Article 4(7), (8).

2. Members Act as Controllers

In the context of threat information sharing, each Member acts as a separate data controller. Members often process threat information differently than FS-ISAC, and for its own specific purposes. Although these purposes may be very similar across the ISAC Membership, the purposes are guided separately by each Member's own specific interests and priorities.

Except for the procedures recorded in FS-ISAC's Operating Rules, which include the requirements of Article 28, a Member sharing information with FS-ISAC does not stipulate how any personal data contained within that threat information should be processed or used by the other Members. Thus, when a Member receives threat information from FS-ISAC, except for the requirements set forth in FS-ISAC's Operating Rules, each Member may process and use that information in accordance with its own internal policies and procedures, including with regard to where that information is stored and how it is processed going forward. As such, each Member processes data as a separate data controller.

In circumstances where FS-ISAC also acts as a data controller, both the Members and FS-ISAC act as independent data controllers, not as joint-controllers. Many Members do not otherwise process the personal data of EU citizens, and therefore are not generally required to comply with GDPR's requirements or run full-scale GDPR compliance programs. However, where FS-ISAC or a Member outside the EU is processing personal data in threat information as an independent data controller, sharing by these Members would be governed by the Controller-to-Controller EU Model Clauses incorporated into FS-ISAC's Operating Rules.40

IV. ISAC Threat Information Sharing Is Lawful Under GDPR

A. Article 6(1)(f) Allows Processing of Personal Data in Threat Information

To process personal data lawfully, data controllers must possess a lawful basis as prescribed under GDPR. Article 6 of the GDPR enumerates the lawful bases upon which data controllers may process personal data. For threat information sharing, Article 6(1)(f) provides a lawful basis for processing personal data contained in threat information.

FS-ISAC

Threat Information Sharing and GDPR

In threat information sharing, both the sharing and receiving party each must possess a lawful basis to process any personal data contained within the threat information being shared. Unless the data is shared peer-to-peer by Members, FS-ISAC, when acting as a data controller, also must possess a lawful basis for processing any personal data within the shared threat information. Article 6 provides an exhaustive list of lawful grounds for processing personal data. Superficially, Article 6(1)(f) provides a lawful basis for FS-ISAC, its Members, and for other ISACS and their members. Article 6(1)(f) states "processing shall be lawful if the:

processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data

40 Although for applicable personal data, Members must comply with the Model Clauses incorporated into the FS-ISAC Operating Rules, when processing personal information in threat information, such Members often are not subject to GDPRdirectly.

subject which require protection of personal data, in particular where the data subject is a child.41

Thus, this Article provides a three-step test – necessity, legitimacy, and balancing interests – for determining the lawfulness of processing of personal data. As stated expressly in the provision, Article 6(1)(f) does not consider the interests pursued by the data controller as the sole calibration of lawfulness. Instead, GDPR considers the legitimacy of the interests pursued by the data controller "or by a third party" for determining whether the processing of personal data is lawful.

In the context of threat information sharing, the interests of FS-ISAC, its Members, as well as the interests of governments, data subjects, and the general public are relevant for determining the lawfulness of the processing. Indeed, each interest is aligned, as articulated in FS-ISAC's mission statement:

To help assure the resilience and continuity of the global financial services infrastructure and individual firms against acts that could significantly impact the [financial] sector's ability to provide services critical to the orderly functioning of the global economy.

These interests, and also the interests of data subjects who are customers of financial firms, and the necessity, individually and collectively, render the processing of personal data in threat information lawful. The interests are legitimate as illustrated by both the guidance of the Article 29 Working Party and the GDPR Recitals. The processing and sharing of personal data in threat information is strictly necessary and proportionate to achieve these purposes behind the legitimate interests, including the prevention of fraud and ensuring network and information security. The processing also satisfies the balancing test under Article 6(1)(f).

1. A29WP's Guidance Shows that the Interests Are Legitimate

Guidance from the Article 29 Working Party illustrates the legitimacy of the interests of FS-ISAC, its Members, governments, and the public, individually and collectively. Under the Article 29 Working Party's guidance on legitimate interests, an interest is "legitimate" if the interest is:

- lawful (i.e., in accordance with applicable EU and national law);
- sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e., sufficiently specific); and
- represents a real and present interest (i.e., it is not speculative).42

lawful (i.e., in accordance with applicable EU and national law);

sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e., sufficiently specific); and

represents a real and present interest (i.e., it is not speculative).42

41 GDPR, Article 6(1)(f) (emphasis added). Other bases may apply to make the processing of personal data by FS-ISAC and its Members lawful under GDPR. However, this paper focuses solely on the basis under Article 6(1)(f).

42 Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (hereinafter "The A29WP Opinion"), available at: **http://ec.europa.eu/justice/article- 29/documentation/opinion-recommendation/files/2014/wp217_en.pdf** at 25. Although The A29WP Opinion pre-dates the GDPR, it still provides a sound explanation of legitimate interests and key issues to consider.

The interests of FS-ISAC and its Members in processing personal data in threat information meets this criteria. First, the interests are lawful. Threat information sharing is exercised pursuant to specific directives in the United States. Indeed, ISACs originally were created by Presidential Executive Order (EO) in response to two significant terrorist attacks occurring in the United States. ISACs, as defined by EO 12472 and the national critical infrastructure protection goals of Presidential Decision Directive 63 (PDD-63), are essential drivers of effective cybersecurity collaboration for specific industrial sectors such as banking and financial services, energy, and telecommunications. More recently, EO 13691 issued under the Obama administration "promotes private sector cybersecurity information sharing" to respond to specific emerging cyber threats.43 The same holds true in the EU. For example, a central tenet of the NIS Directive is to support and facilitate strategic cooperation and the exchange of information by Member States, including by creating a Cooperation Group and a network of national CSIRTs.44 Information sharing is also promoted at a national Member State level. For example, the UK Cyber Security Information Sharing Partnership (CISP), is a joint UK government and industry initiative set up to exchange cyber threat information in real time. As threat information sharing, including that already performed in the EU, remains subject to international laws (including those outlined above) it follows that it is carried out legally (subject to compliance with GDPR requirements). Second, the interests can be clearly articulated to allow the Article 6(1)(f) balancing test (discussed in Section VI.4. below) between them and the fundamental rights of the data subject to be protected. FS-ISAC's mission is to "help assure the resilience and continuity of the global financial services infrastructure[.]" The goals and purposes of threat information sharing are to preserve networks, systems, and associated personal data from unauthorized acquisition, alteration, or loss. If networks and systems do not have adequate security and protection, the privacy of personal data in those networks and systems cannot be secured and maintained. Finally, the interests are real and ever-present. It has become critical for organizations to share threat information as part of their resiliency and security program given the growing sophistication of threat actors and their techniques to trigger cyberattacks, and the ever-expanding interconnectivity of global networks. There are also broad and important interests of the general public for detecting and preventing criminal activity, like financial and consumer fraud, and protecting critical financial infrastructure. The global threat of cyberattacks and financial fraud is ongoing, and the activities of FSISAC are known to be effective in the protection of financial institutions and networks from cyberattacks.

2. GDPR Recitals Demonstrate the Legitimacy of the Processing

The GDPR itself expressly shows that the purposes of processing personal data contained within threat information constitute a legitimate interest. Under GDPR Recitals 47, 49 and 50, certain expressed purposes of processing of personal data may constitute a legitimate interest. These purposes are: fraud prevention; ensuring network and information security; and indicating possible

43 See Cyber Threat Intelligence, ISAOs, available at **https://ctin.us/site/isaos/.**

44 See Section III.B. above

criminal acts or threats to public security. FS-ISAC and its Members process personal data contained within threat information for all three of these purposes.

a. Fraud Prevention

Recital 47 of GDPR states that the legitimate interests of a data controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing personal data so long as those interests are not outweighed by the interests or fundamental rights and freedoms of the data subject. An included example of whether the processing of personal data constitutes a legitimate interest of the data controller is where "the processing of personal data [is] strictly necessary for the purposes of preventing fraud[.]" The interests of FS-ISAC and its Members, as data controllers, fall squarely within this recital.

Much of the threat information shared by FS-ISAC and its Members is shared with a primary aim of preventing fraudulent activity. For example, FS-ISAC and its Members may share Stolen/Victim Personal Data with other Members or Law Enforcement to prevent further fraud and harm suffered by the data subject whose personal data was stolen and is being misused. FS-ISAC and its Members may share Threat Actor Personal Data with Members or authorities to prevent further crimes and to bring threat actors to justice under EU law or the law of other jurisdictions.

b. Network and Information Security

Recital 49 of GDPR states that "processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, including the ability to prevent "unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data," or the "security of the related services" offered or accessible via those networks and systems, "constitutes a legitimate interest of the data controller[.]" The interests of FS-ISAC and its Members, as data controllers, also fall within this recital.

FS-ISAC and its Members process threat information for the purpose of resisting "unlawful or malicious actions" of those who seek to compromise the security of financial institutions' networks and systems to "compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data" therein. For example, FS-ISAC's mission statement states that the purpose of FS-ISAC's information sharing is to "help assure the resilience and continuity of the global financial services infrastructure and individual firms against acts that could significantly impact the [financial] sector's ability to provide services critical to the orderly functioning of the global economy."45 These interests protect the general public, providing stability and reliability in local, national, and international commerce.

45 Although FS-ISAC and its Members do not fall squarely within the specified categories of data controllers listed in Recital

49 (i.e., CERTs or CSIRTs), FS-ISAC and its Members process personal data in threat information sharing for the very purposes described in Recital 49. Also, arguably "providers of electronic communications networks and services and by providers of security technologies and services" referenced in Recital 49 with CERTs and CSIRTs encompass by close analogy financial institutions constituting the global financial services network infrastructure.

c. Identifying Possible Criminal Activity or Threats to Public Security

Recital 50 of GDPR states that the "processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected." Included in examples of such "compatible" processing is "[i]ndicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority[.]" Again, the interests of FS-ISAC and its Members as data controllers also fall squarely within this recital.

FS-ISAC was established to share information about threats to the financial services sector's infrastructure and stability, including information about any malicious acts that might diminish the ability of a government to ensure public health and safety. It assists approximately 7,000 member firms to reduce their organizational and systemic risk from various types of threats through information sharing, establishing best practices, and collaborating from the analyst level to the CEO level. To support this mission, FS-ISAC and its Members share threat information with government agencies and law enforcement departments. FS-ISAC has formal cooperation agreements with government and law enforcement agencies around the world, and maintains a wide variety of relationships with reputable, capable organizations. It also strictly follows TLP, and does not share any information that is provided by a member with any non-member organization unless the member specifically requests otherwise. Members may ask for help sharing information, anonymously or with attribution, with FS-ISACconnected law enforcement agencies, CERTs/CSIRTs, and other relevant government entities.

3. The Processing is Strictly Necessary and Proportionate

Under Article 6(1)(f), the processing of personal data must be necessary and proportionate to the pursuit of the legitimate interest.46 To be necessary, or strictly necessary, there must be no viable or practical alternative method to achieve the purpose behind the interest, such as the prevention of fraud.47 For example, the controller should satisfy itself that it is not possible to achieve the relevant purpose in another more obvious or less intrusive way. In the context of threat information sharing, the processing of personal data contained in threat information is likely to be considered strictly necessary and proportionate, and thereby satisfies the criteria of necessity under Article 6(1)(f).

The processing of personal data is very likely to be considered strictly necessary. This is because threat information sharing, and the processing of personal data therein, is a critical and proven component of ensuring network and system security. In particular, sharing certain personal data (such as IP or email addresses) can prove to be "essential" in rapidly identifying, flagging, preventing, and countering security breaches or the exploitation of discovered vulnerabilities, such as phishing attacks, malware, and denial of service attacks.48 For example, the processing of Threat Actor Personal Data

46 As outlined in the previous section, the fraud prevention and network and security purposes go one step further and require the processing to be 'strictly necessary and proportionate' for the purpose it is seeking to achieve.

47 The A29WP Opinion, at 55.

48 Cormack, Incident Response: Protecting Individual Rights Under GDPR, at 271; see also S. Bradshaw, "Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity" (2015), at 11, available at

https://www.cigionline.org/sites/default/files/gcig_no23web_0.pdf.

relating to an unsuccessful cyber incident against one Member, can help additional Members secure their own systems against cyber threats from that same individual. Similarly, sharing Stolen/Victim Personal Data within the Member community is the quickest, and most efficient and effective, way for Members to prevent a data subject from being a victim of further fraud or criminal activity. Indeed, it is the real-time, collaborative sharing of accurate, relevant and localised information between financial organizations that differentiates the threat sharing model as an effective, insightful and unique tool for successfully improving an organization's security posture. No alternative method currently exists which would deliver the same security and fraud prevention outcomes within such tight timeframes. Similarly, any attempt to remove personal data from the threat information that is shared, would prove disproportionately onerous, undermine the value of the insight for organizations, and cut across the very purpose of threat sharing, thereby making network security unfeasible.49 The processing of such personal data is likely to be considered proportionate. Given the weight of the interests of FS-ISAC and its Members, as well as that of governmental entities and the public at large, information sharing, and its impact on data subjects, is neither excessive, unwarranted or out of step with the valuable purposes pursued. In fact, the interests are not diametrically opposed, but instead are complementary.50 The processing is also consistent with the interests pursued by FS-ISAC and its Members to protect personal data. In addition, threat information sharing conducted by ISACs, including FS-ISAC and its Members, is adequately targeted and controlled to meet objectives, while minimizing the impact on data subjects. For example, TLP measures and restricts the use and dissemination of threat information based upon, among other considerations, the sensitivity of the information, its reliability, and the nature of the threat identified. FS-ISAC (and other ISACs) also do not process personal data to take action against the data subjects. Instead, threat information, including any personal data therein, is processed to enable FS-ISAC's Members and/or other organizations to improve security and withstand possible or anticipated cyberattacks.

4. The Balancing Test Under Article 6

Finally, the lawfulness of processing personal data by FS-ISAC under Article 6(1)(f) satisfies the Article 6 balancing test that weighs the legitimate interests of the controller or the third party against the interests and fundamental rights and freedoms of the data subject. In the context of threat information sharing and the categories of personal data processed in threat information, the processing of such personal data is not and would not be overridden by the interests of the data subjects whose data is processed.

a. The Legitimate Interests of FS-ISAC and Its Members Are Not Outweighed

The legitimate interests of FS-ISAC and its Members would not be outweighed by the interests or rights of the data subject, especially when considering the types of personal data contained in threat information. For instance, the processing of Stolen/Victim Personal Data to prevent further fraudulent

49 E.g., Silva and Coudert, ACDC – Legal Requirements, at 56 (noting "need for cooperation and information sharing" to combat cybercrime and cyber threats "is crucial").

50 Silva and Coudert, ACDC – Legal Requirements, at 40 (discussing proportionality test under Article 7(f) of Directive EC 95/46 weighing the legitimate interests against the need to protect data subjects' fundamental rights of confidentiality.

crimes against that data subject would not be overridden by the data subject's interests. A data subject who has had his or her personal data stolen could be a victim of fraud, identify theft, or other crimes. FS-ISAC's processing of Stolen/Victim Personal Data would not impose a detrimental effect upon the data subject's rights or interests, but would benefit them and the data subject. Additionally, the processing could stop further identity theft and harm to the data subject, or help validate the theft's occurrence to give the data subject avenues for restitution and recovery. Nor would the interests of threat actors override the processing of personal data contained in threat information by FS-ISAC and its Members. The Article 29 Working Party's guidance on legitimate interests is illustrative. There, the Article 29 Working Party stressed the importance of considering both the interests of data subjects and their rights and freedoms, stating that if a data controller may pursueany legitimate interest, then "the data subject should also be entitled to have all categories of interests to be taken into account and weighed against those of the controller."51 Yet, when a data subject is engaged in illegal activity, although his or her interests should not be disregarded, the Article 29 Working Party stated that any interference with a threat actor's rights and interests simply must not be "disproportionate":

Even individuals engaged in illegal activities should not be subject to disproportionate interference with their rights and interests. For example, an individual who may have perpetrated theft in a supermarket could still see his interests prevailing against the publication of his picture and private address on the walls of the supermarket and/or on the Internet by the owner of the shop.52

Threat information sharing is not punitive. It is not predatory or vindictive. The purpose of threat information sharing is to prevent crime, and ultimately to protect data subjects from harm. Processing personal data of threat actors (i.e., Threat Actor Personal Data) contained in threat information by FSISAC and its Members to stop fraud, to identify theft, or to enhance network security would not be disproportionate in any manner to a threat actor's interests. In addition, those interests are further protected by the use of TLP measures adopted to treat information in a manner appropriate to its sensitivity.

Thus, because FS-ISAC and its Members restrict dissemination of threat information, including personal data contained therein, under TLP for the purposes of preventing crime and ensuring network security, any sharing of Threat Actor Personal Data or Falsified Personal Data used by a threat actor to evade detection and to further a criminal conspiracy, with other financial institutions to ward off an attack, or to authorities to assist with an arrest, is proportionate to the perceived threat. Threat information sharing is not akin to the Article 29 Working Party's example of publishing a photo and 51 A29WP Opinion at 30. 52 Id. at 30 (emphasis added).

private address of a thief on the Internet, an action that exhibits punitive and arbitrary qualities.53 Under the Article 29 Working Party guidance, the outcome of a balancing test should weigh in favor of FSISAC and its Members.

b. Other Factors Illustrate the Legitimate Interests Are Not Outweighed

There are additional factors to consider when conducting a balancing test to further illustrate the lawfulness of processing personal data in threat information by FS-ISAC and its Members under Article 6(1)(f). Those factors are: the nature of the personal data being processed; the reasonable expectations of the individual data subjects; the likely impact of the processing on the individual; and whether any safeguards can be put in place to mitigate negative impacts.

(I) Nature of the Personal Data

Typically, in the context of threat information sharing, the types of personal data being processed are not intrusive, and in fact would provide great weight to the interests or rights of the data subject. The majority of personal data processed and shared in threat information includes IP addresses (or other online identifiers) of threat actors. Such data is not special, sensitive or particularly personal. Other personal data may be bank details of victims, but such information usually is shared to prevent further fraud on those victims.54

(II) The Data Subjects' Reasonable Expectations

An objective test, the data subject's reasonable expectations, requires that a reasonable person in the data subjects' position would expect the processing of their personal data in light of the particular circumstances. In its guidance, the Article 29 Working Party opined that "the more compelling the interest of the controller, and the more clearly acknowledged and expected it is in the wider community that the controller may take action and process data in pursuit of such an interest, the more heavily this legitimate interest weighs in the balance."55 Thus, a data subject's reasonable expectations is lowered in instances where the data controller has a compelling interest to process the personal data and the community anticipates that the controller may take action and process the data in pursuit of its interest.

In the context of threat information sharing, FS-ISAC and its Members, as data controllers, have compelling interests that are clearly acknowledged and e xpected in the wider community: the prevention of fraud, ensuring network security against cyberattacks, and the possible identification of criminal activity or threats to the public. Thus, it is reasonable to assert that both victims and threat

53 The Information Commissioner's Office ("ICO"), the supervisory authority responsible for data protection law enforcement in the UK, has stated in its own guidance that processing personal data for the purpose of achieving network and information security is a strong factor in the balancing test. Although this guidance is not applicable to all EU Member States, it provides a good indication that processing data for network security is strongly favoured in a balancing test. The ICO also believes that in many circumstances, conducting a balancing test could be relatively brief. See ICO Guidance on Legitimate Interests, available at:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/.

54 The processing of personal data categorized as special under Article 9 admittedly could be considered more intrusive and pose a greater risk to a data subject's rights and freedoms. However, it is highly unlikely that any personal data processed by FS-ISAC and its Members would constitute a special category of personal data.

55 A29WP Opinion at 35.

actors reasonably would expect that banks and other financial institutions share personal information for the purposes of fraud protection, ensuring network and information security, and identifying possible criminal activity. Indeed, it is one reason why threat actors use Falsified Personal Data – to conceal their identity when financial institutions process personal data. Further, the broader community expects banks and other financial institutions to take such action for those purposes.

(III) Impact on Data Subjects

The Article 29 Working Party has clarified that when assessing the impact of processing on data subjects, both negative and positive consequences should be taken into account.56 The consequences of FS-ISAC and its Members processing personal data are positive and proportionate.
In the context of threat information sharing, the impact of processing Stolen/Victim Personal Data would be positive. For data subjects whose personal data has been stolen and who are victims of crime, the sharing of data can prevent further fraud against the victim and the community at large. It also may assist with providing the victim with relief and restitution. For threat actors, the potential impact on their rights and freedoms is more significant, as processing could ultimately lead to their arrest or imprisonment. However, the Article 29 Working Party opined that individuals engaged in illegal activities "should not be subject to disproportionate interference with their rights and interests."57 Processing personal data to prevent further crime, permit law enforcement to protect the security of financial institutions' networks and systems – and the personal data contained therein – and to permit restitution for victims, is not disproportionate – even if it means an arrest of the threat actor to subject him or her to the process of the EU Member State's judicial process. Threat information sharing is not intended for punitive purposes. The intent of threat information sharing is to protect systems and networks, and the personal data contained therein.

(IV) Safeguards Undertaken by FS-ISAC and its Members

The potential negative impact on data subjects caused by processing their personal data may be reduced if the data controller undertakes measures to protect and secure the personal data, thereby providing greater weight to the processing of the data. FS-ISAC and its Members undertake safeguards to protect the personal data they process in threat information. The Article 29 Working Party clarified that "it is important to highlight the special role that safeguards may play in reducing the undue impact on the data subjects, and thereby changing the balance of rights and interests to the extent that the data controller's legitimate interests will not be overridden."58 Safeguard measures employed by FS-ISAC and its Members include encryption, annual cybersecurity assessments and robust cybersecurity programs aimed at early detection and mitigation of cyber events, as well as other cybersecurity tools and processes. FS-ISAC and its Members also adhere to TLP to restrict the dissemination of threat information when shared between Members. These safeguards help to provide further weight to processing performed by FS-ISAC and its Members when

56 Id. at 37.
57 Id. at 30 (emphasis added).
58 Id. at 31.

balancing their respective legitimate interests against the interests of data subjects.

V. Conclusion

Because the purposes and goals of information threat sharing serve to advance the fundamental tenets of GDPR, the processing of personal data contained within threat information should comply with and fall squarely within Article 6(1)(f). The processing of such personal data is necessary for the legitimate interests pursued by FS-ISAC and its Members as data controllers, namely to prevent crime aimed against financial services organizations, and to ensure network security and the protection of personal data held by those financial organizations. For the same reasons, the processing also is necessary for the legitimate interests of third parties, including governmental entities and law enforcement, the public at large, and the data subjects whose personal data may be targeted and misused by a threat actor.

The processing of the personal data also satisfies Article 6(1)(f)'s balancing test. The legitimate interests of FS-ISAC and its Members are not outweighed by the rights and interests of the data subjects whose personal data is processed. In the case of stolen personal data, the processing of such information benefits the data subjects because it could prevent or stop fraud being committed against them and help lead them to recovery. For threat actors, the processing of their personal data is not disproportionate to the legitimate interests being served. Additional factors weighing in further favor of the processing include the nature of the personal data itself (i.e., stolen data and data of the malicious threat actor), reasonable expectations that FS-ISAC and its Members seek to prevent fraud and cyberattacks, the positive impact of threat information sharing to ensure security and the protection of personal data, and the protective measures taken by FS-ISAC and its Members under TLP.

Thus, threat information sharing seeks to preserve fundamental goals of GDPR, and is a cornerstone to the regulation's principles and purpose: to protect "fundamental rights and freedoms of natural persons and in particular their right to protection of personal data."

FS-ISAC

Threat Information Sharing and GDPR

About the Authors

Richard M. Borden | Partner and Chief Privacy Officer, White and Williams LLP

Mr. Borden is at the forefront of cybersecurity and privacy issues. He focuses his practice on big data governance and the Internet of Things, cybersecurity risk management, and technology sourcing and transactions. A Certified Information Privacy Professional/US, Mr. Borden can translate the often
complicated language of technology, cybersecurity, privacy, risk and compliance so that it's understood from both a legal and business perspective. His experience on both the customer and vendor side enables him to advise general counsel, C-Suite executives and boards of directors on understanding potential risks and incident response. Mr. Borden serves as editor for an initiative launched by the Accredited Standards Committee X9 Inc. The X9.141 Financial and Personal Data Protection and Breach Notification Standard will provide management and security requirements to protect personal and financial data and to detect, respond to and mitigate data breaches.

Joshua A. Mooney | Partner and Co-Chair, Cyber Law and Data Protection Group, White and Williams LLP

Mr. Mooney advises corporate clients on matters involving cyber risk, data protection and privacy. He assists with the development and implementation of data privacy and security programs under GDPR, the New York cyber regulations, and other regulatory frameworks. He also guides clients through investigations and responses to cybersecurity incidents, including personal data breaches. Mr. Mooney currently serves as editor for an initiative launched by the Accredited Standards Committee X9 to develop a universal standard for data protection and data breach notification in the financial services industry. In addition, he advises insurance carriers on emerging coverage risks involving cyber and privacy rights, including data breaches, malware and social engineering, e-surveillance, TCPA, and invasion of privacy. Mr. Mooney has been quoted in The Wall Street Journal, Law360, and Business Insurance. He is the Chair of the Pennsylvania Bar Association's Cybersecurity and Data Privacy Committee. Mr. Mooney also is a member of the ABA TIPS Cybersecurity and Data Privacy Committee, where he serves as Vice-Chair. Outside of White and Williams, Mr. Mooney has been designated as "convener" for Cambridge University alumni in the Commonwealth of Pennsylvania.

Mark Taylor | Partner, Osborne Clarke LLP

Mr. Taylor is a partner in Osborne Clarke's London office with extensive experience in technology and data protection matters. He has particular expertise advising clients in the financial services and digital business sectors, and regularly advises clients on a wide range of data protection and cybersecurity issues. Mr. Taylor also advises clients on FinTech matters, digital payments, encryption and interception of communications issues. Mr. Taylor is a Trustee of the Society for Computers and Law, and is the Technology section editor of Computers and Telecommunications Law Review. Prior to becoming a lawyer, Mr. Taylor worked for IBM writing and developing software.

Matthew Sharkey | Senior Associate, Osborne Clarke LLP

Matthew is a Senior Associate in Osborne Clarke's London office, where he focuses on matters relating to information technology and data protection. He is experienced in advising on data protection and IT security matters, as well as electronic signatures, digital payments, large-scale outsourcing projects and a broad range of technology contracts and issues.